Controlar el acceso a StorageGRID

StorageGRID software

NetApp
December 03, 2025

Tabla de contenidos

Controlar el acceso a StorageGRID

Controlar el acceso a StorageGRID

Usted controla quién puede acceder a StorageGRID y qué tareas pueden realizar los usuarios creando o importando grupos y usuarios y asignando permisos a cada grupo. Opcionalmente, puede habilitar el inicio de sesión único (SSO), crear certificados de cliente y cambiar las contraseñas de la red.

Controlar el acceso al Administrador de Grid

Usted determina quién puede acceder al Administrador de Grid y a la API de Administración de Grid importando grupos y usuarios desde un servicio de federación de identidad o configurando grupos y usuarios locales.

Usando"federación de identidades" facilita la configuración"grupos" y"usuarios" es más rápido y permite a los usuarios iniciar sesión en StorageGRID usando credenciales familiares. Puede configurar la federación de identidad si utiliza Active Directory, OpenLDAP u Oracle Directory Server.

> Comuníquese con el soporte técnico si desea utilizar otro servicio LDAP v3.

Usted determina qué tareas puede realizar cada usuario asignándoles diferentes"permisos" a cada grupo. Por ejemplo, es posible que desee que los usuarios de un grupo puedan administrar las reglas de ILM y que los usuarios de otro grupo puedan realizar tareas de mantenimiento. Un usuario debe pertenecer al menos a un grupo para acceder al sistema.

Opcionalmente, puede configurar un grupo para que sea de solo lectura. Los usuarios de un grupo de solo lectura solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de Grid ni en la API de administración de Grid.

Habilitar el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0). Después de usted"configurar y habilitar SSO" Todos los usuarios deben estar autenticados por un proveedor de identidad externo antes de poder acceder al Administrador de Grid, al Administrador de Inquilinos, a la API de Administración de Grid o a la API de Administración de Inquilinos. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cambiar la contraseña de aprovisionamiento

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para descargar el paquete de recuperación de StorageGRID . La frase de contraseña también es necesaria para descargar copias de seguridad de la información de topología de la red y de las claves de cifrado para el sistema StorageGRID . Puede"cambiar la contraseña" según sea necesario.

Cambiar las contraseñas de la consola del nodo

Cada nodo de su red tiene una contraseña de consola de nodo única, que necesita para iniciar sesión en el nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. Según sea necesario, puede"cambiar la contraseña de la consola del nodo" para cada nodo.

Cambiar la contraseña de aprovisionamiento

Utilice este procedimiento para cambiar la frase de contraseña de aprovisionamiento de StorageGRID . La frase de contraseña es necesaria para los procedimientos de recuperación, expansión y mantenimiento. La frase de contraseña también es necesaria para descargar copias de seguridad del paquete de recuperación que incluyen la información de topología de la red, las contraseñas de la consola del nodo de la red y las claves de cifrado para el sistema StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tiene permisos de acceso de mantenimiento o root.
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

La frase de contraseña de aprovisionamiento es necesaria para muchos procedimientos de instalación y mantenimiento, y para"descargando el paquete de recuperación" . La frase de contraseña de aprovisionamiento no aparece en la `Passwords.txt` archivo. Asegúrese de documentar la contraseña de aprovisionamiento y guardarla en un lugar seguro.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso**> **Contraseñas de red**.
2. En **Cambiar contraseña de aprovisionamiento**, seleccione **Realizar un cambio**
3. Introduzca su contraseña de aprovisionamiento actual.
4. Introduzca la nueva contraseña. La frase de contraseña debe contener al menos 8 y no más de 32 caracteres. Las frases de contraseña distinguen entre mayúsculas y minúsculas.
5. Guarde la nueva contraseña de aprovisionamiento en una ubicación segura. Es necesario para procedimientos de instalación, expansión y mantenimiento.
6. Vuelva a ingresar la nueva contraseña y seleccione **Guardar**.

   El sistema muestra un banner de éxito verde cuando se completa el cambio de contraseña de aprovisionamiento.

7. Seleccione **Paquete de recuperación**.
8. Ingrese la nueva contraseña de aprovisionamiento para descargar el nuevo paquete de recuperación.

> Después de cambiar la contraseña de aprovisionamiento, debe descargar inmediatamente un nuevo paquete de recuperación. El archivo del paquete de recuperación le permite restaurar el sistema si ocurre una falla.

Cambiar las contraseñas de la consola del nodo

Cada nodo de su red tiene una contraseña de consola de nodo única, que necesita para

iniciar sesión en el nodo. Utilice estos pasos para cambiar la contraseña única de la consola de cada nodo de su red.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de mantenimiento o acceso root" .
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

Utilice la contraseña de la consola del nodo para iniciar sesión en un nodo como "admin" mediante SSH, o como usuario root en una conexión de consola física/VM. El proceso de cambio de contraseña de la consola del nodo crea nuevas contraseñas para cada nodo de su red y almacena las contraseñas en un archivo actualizado. `Passwords.txt` archivo en el paquete de recuperación. Las contraseñas aparecen en la columna Contraseña del archivo Passwords.txt.

> Hay contraseñas de acceso SSH independientes para las claves SSH utilizadas para la comunicación entre nodos. Las contraseñas de acceso SSH no se modifican con este procedimiento.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Contraseñas de red**.
2. En **Cambiar contraseñas de la consola del nodo**, seleccione **Realizar un cambio**.

Introduzca la contraseña de aprovisionamiento

Pasos

1. Introduzca la contraseña de aprovisionamiento para su red.
2. Seleccione **Continuar**.

Descargar el paquete de recuperación actual

Antes de cambiar las contraseñas de la consola del nodo, descargue el paquete de recuperación actual. Puede utilizar las contraseñas de este archivo si el proceso de cambio de contraseña falla para algún nodo.

Pasos

1. Seleccione **Descargar paquete de recuperación**.
2. Copiar el archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

3. Seleccione **Continuar**.
4. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las contraseñas de la consola del nodo.

   No puedes cancelar este proceso una vez iniciado.

Cambiar las contraseñas de la consola del nodo

Cuando se inicia el proceso de contraseña de la consola del nodo, se genera un nuevo paquete de recuperación que incluye las nuevas contraseñas. Luego, las contraseñas se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Seleccione **Descargar nuevo paquete de recuperación**.
3. Cuando se complete la descarga:

   a. Abrir el `.zip` archivo.

   b. Confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo, que contiene las nuevas contraseñas de la consola del nodo.

   c. Copiar el nuevo archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

   > No sobrescriba el paquete de recuperación antiguo.

   El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Seleccione la casilla de verificación para indicar que ha descargado el nuevo paquete de recuperación y verificado el contenido.
5. Seleccione **Cambiar contraseñas de la consola del nodo** y espere a que todos los nodos se actualicen con las nuevas contraseñas. Esto podría tardar unos minutos.

   Si se cambian las contraseñas de todos los nodos, aparece un banner de éxito verde. Vaya al siguiente paso.

   Si se produce un error durante el proceso de actualización, aparecerá un mensaje con la lista de nodos que no pudieron cambiar sus contraseñas. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya contraseña no se haya podido cambiar. Si el proceso finaliza con algunos nodos que aún no tienen la contraseña cambiada, aparece el botón **Reintentar**.

   Si la actualización de contraseña falló para uno o más nodos:

   a. Revise los mensajes de error enumerados en la tabla.

   b. Resolver los problemas.

   c. Seleccione **Reintentar**.

   > Al volver a intentarlo solo se cambian las contraseñas de la consola de nodo en los nodos que fallaron durante intentos anteriores de cambio de contraseña.

6. Después de cambiar las contraseñas de la consola de nodo para todos los nodos, elimine el archivoprimer paquete de recuperación que descargaste .
7. Opcionalmente, utilice el enlace **Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Cambiar las contraseñas de acceso SSH para los nodos de administración

Al cambiar las contraseñas de acceso SSH para los nodos de administración también se actualizan los conjuntos únicos de claves SSH internas para cada nodo de la red. El nodo de administración principal utiliza estas claves SSH para acceder a los nodos mediante una autenticación segura y sin contraseña.

Utilice una clave SSH para iniciar sesión en un nodo como `admin` o al usuario root en una máquina virtual o conexión de consola física.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de mantenimiento o acceso root" .
- Tienes la contraseña de aprovisionamiento actual.

Acerca de esta tarea

Las nuevas contraseñas de acceso para los nodos de administración y las nuevas claves internas para cada nodo se almacenan en el `Passwords.txt` archivo en el paquete de recuperación. Las claves se enumeran en la columna Contraseña de ese archivo.

Hay contraseñas de acceso SSH independientes para las claves SSH utilizadas para la comunicación entre nodos. Estos no se modifican con este procedimiento.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Contraseñas de red**.
2. En **Cambiar claves SSH**, seleccione **Realizar un cambio**.

Descargar el paquete de recuperación actual

Antes de cambiar las claves de acceso SSH, descargue el paquete de recuperación actual. Puede utilizar las claves de este archivo si el proceso de cambio de clave falla para algún nodo.

Pasos

1. Introduzca la contraseña de aprovisionamiento para su red.
2. Seleccione **Descargar paquete de recuperación**.
3. Copiar el archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

> El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Seleccione **Continuar**.
5. Cuando aparezca el cuadro de diálogo de confirmación, seleccione **Sí** si está listo para comenzar a cambiar las claves de acceso SSH.

No puedes cancelar este proceso una vez iniciado.

Cambiar las claves de acceso SSH

Cuando se inicia el proceso de cambio de claves de acceso SSH, se genera un nuevo paquete de recuperación que incluye las nuevas claves. Luego, las claves se actualizan en cada nodo.

Pasos

1. Espere a que se genere el nuevo paquete de recuperación, lo que puede tardar unos minutos.
2. Cuando el botón Descargar nuevo paquete de recuperación esté habilitado, seleccione **Descargar nuevo paquete de recuperación** y guarde el archivo del nuevo paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.
3. Cuando se complete la descarga:

   a. Abrir el `.zip` archivo.

   b. Confirme que puede acceder al contenido, incluido el `Passwords.txt` archivo, que contiene las nuevas claves de acceso SSH.

   c. Copiar el nuevo archivo del paquete de recuperación(`.zip`) a dos lugares seguros, protegidos y separados.

      No sobrescriba el paquete de recuperación antiguo.

   El archivo del paquete de recuperación debe estar protegido porque contiene claves de cifrado y contraseñas que se pueden utilizar para obtener datos del sistema StorageGRID .

4. Espere a que las claves se actualicen en cada nodo, lo que puede demorar unos minutos.

   Si se cambian las claves de todos los nodos, aparece un banner de éxito verde.

   Si se produce un error durante el proceso de actualización, un mensaje de banner enumera la cantidad de nodos cuyas claves no se pudieron cambiar. El sistema volverá a intentar automáticamente el proceso en cualquier nodo cuya clave no haya sido cambiada. Si el proceso finaliza con algunos nodos que aún no tienen una clave modificada, aparece el botón **Reintentar**.

   Si la actualización de la clave falló para uno o más nodos:

   a. Revise los mensajes de error enumerados en la tabla.

   b. Resolver los problemas.

   c. Seleccione **Reintentar**.

      Al volver a intentarlo solo se cambian las claves de acceso SSH en los nodos que fallaron durante intentos de cambio de clave anteriores.

5. Después de cambiar las claves de acceso SSH para todos los nodos, elimine el archivoprimer paquete de recuperación que descargaste .
6. Opcionalmente, seleccione **MANTENIMIENTO** > **Sistema** > **Paquete de recuperación** para descargar una copia adicional del nuevo paquete de recuperación.

Utilizar la federación de identidades

El uso de la federación de identidades agiliza la configuración de grupos y usuarios, y permite a los usuarios iniciar sesión en StorageGRID usando credenciales familiares.

Configurar la federación de identidades para Grid Manager

Puede configurar la federación de identidad en Grid Manager si desea que los grupos de administradores y los usuarios se administren en otro sistema, como Active Directory, Azure Active Directory (Azure AD), OpenLDAP u Oracle Directory Server.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Está utilizando Active Directory, Azure AD, OpenLDAP u Oracle Directory Server como proveedor de identidad.

> Si desea utilizar un servicio LDAP v3 que no figura en la lista, comuníquese con el soporte técnico.

- Si planea utilizar OpenLDAP, debe configurar el servidor OpenLDAP. Ver Directrices para configurar un servidor OpenLDAP .
- Si planea habilitar el inicio de sesión único (SSO), ha revisado la"Requisitos y consideraciones para el inicio de sesión único" .
- Si planea utilizar Seguridad de la capa de transporte (TLS) para las comunicaciones con el servidor LDAP, el proveedor de identidad utiliza TLS 1.2 o 1.3. Ver "Cifrados compatibles para conexiones TLS salientes" .

Acerca de esta tarea

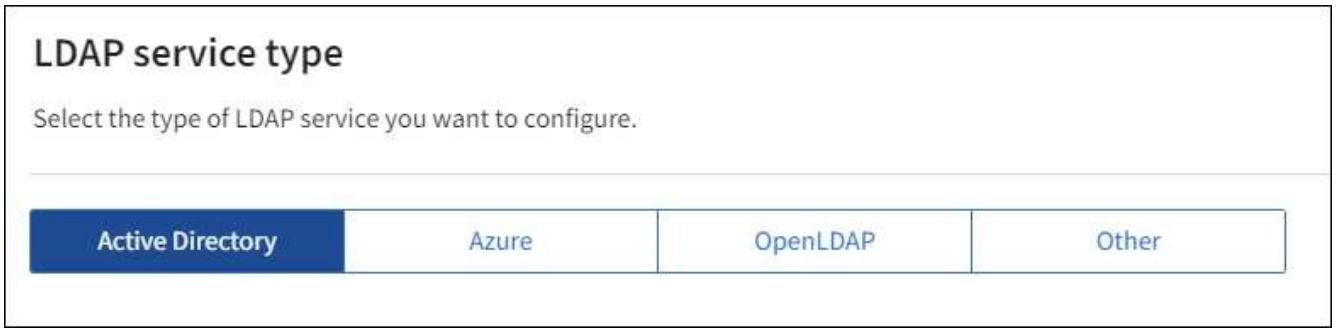
Puede configurar una fuente de identidad para Grid Manager si desea importar grupos desde otro sistema, como Active Directory, Azure AD, OpenLDAP u Oracle Directory Server. Puede importar los siguientes tipos de grupos:

- Grupos de administración. Los usuarios de los grupos de administración pueden iniciar sesión en Grid Manager y realizar tareas, según los permisos de administración asignados al grupo.
- Grupos de usuarios inquilinos para inquilinos que no utilizan su propia fuente de identidad. Los usuarios de los grupos de inquilinos pueden iniciar sesión en el Administrador de inquilinos y realizar tareas, según los permisos asignados al grupo en el Administrador de inquilinos. Ver"Crear una cuenta de inquilino" y"Utilice una cuenta de inquilino" Para más detalles.

Entrar a la configuración

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Federación de identidades**.
2. Seleccione **Habilitar federación de identidad**.
3. En la sección Tipo de servicio LDAP, seleccione el tipo de servicio LDAP que desea configurar.



Seleccione **Otro** para configurar valores para un servidor LDAP que utiliza Oracle Directory Server.

4. Si seleccionó **Otro**, complete los campos en la sección Atributos LDAP. De lo contrario, vaya al siguiente paso.
   - **Nombre único de usuario**: el nombre del atributo que contiene el identificador único de un usuario LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `uid` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `uid` .
   - **UUID de usuario**: el nombre del atributo que contiene el identificador único permanente de un usuario LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid` . El valor de cada usuario para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
   - **Nombre único del grupo**: el nombre del atributo que contiene el identificador único de un grupo LDAP. Este atributo es equivalente a `sAMAccountName` para Active Directory y `cn` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `cn` .
   - **UUID de grupo**: el nombre del atributo que contiene el identificador único permanente de un grupo LDAP. Este atributo es equivalente a `objectGUID` para Active Directory y `entryUUID` para OpenLDAP. Si está configurando Oracle Directory Server, ingrese `nsuniqueid` . El valor de cada grupo para el atributo especificado debe ser un número hexadecimal de 32 dígitos en formato de 16 bytes o de cadena, donde se ignoran los guiones.
5. Para todos los tipos de servicios LDAP, ingrese la información de conexión de red y servidor LDAP requerida en la sección Configurar servidor LDAP.
   - **Nombre de host**: el nombre de dominio completo (FQDN) o la dirección IP del servidor LDAP.
   - **Puerto**: El puerto utilizado para conectarse al servidor LDAP.

     El puerto predeterminado para STARTTLS es 389 y el puerto predeterminado para LDAPS es 636. Sin embargo, puedes utilizar cualquier puerto siempre que tu firewall esté configurado correctamente.

   - **Nombre de usuario**: La ruta completa del nombre distinguido (DN) del usuario que se conectará al servidor LDAP.

     Para Active Directory, también puede especificar el nombre de inicio de sesión de nivel inferior o el nombre principal del usuario.

     El usuario especificado debe tener permiso para enumerar grupos y usuarios y acceder a los siguientes atributos:

     - `sAMAccountName`o `uid`

- `objectGUID`, `entryUUID` , o `nsuniqueid`
- `cn`
- `memberOf`o `isMemberOf`
- **Directorio Activo**: `objectSid` , `primaryGroupID` , `userAccountControl` , y `userPrincipalName`
- **Azur**: `accountEnabled` y `userPrincipalName`

◦ **Contraseña**: La contraseña asociada al nombre de usuario.

> Si cambia la contraseña en el futuro, deberá actualizarla en esta página.

◦ **DN base de grupo**: la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el que desea buscar grupos. En el ejemplo de Active Directory (abajo), todos los grupos cuyo nombre distintivo es relativo al DN base (DC=storagegrid,DC=example,DC=com) se pueden usar como grupos federados.

> Los valores de **Nombre único del grupo** deben ser únicos dentro del **DN base del grupo** al que pertenecen.

◦ **DN base de usuario**: la ruta completa del nombre distinguido (DN) de un subárbol LDAP en el que desea buscar usuarios.

> Los valores de **Nombre único de usuario** deben ser únicos dentro del **DN base de usuario** al que pertenecen.

◦ **Formato de nombre de usuario vinculado** (opcional): el patrón de nombre de usuario predeterminado que StorageGRID debe usar si el patrón no se puede determinar automáticamente.

Se recomienda proporcionar **Formato de nombre de usuario de enlace** porque puede permitir que los usuarios inicien sesión si StorageGRID no puede vincularse con la cuenta de servicio.

Introduzca uno de estos patrones:

- **Patrón UserPrincipalName (Active Directory y Azure)**: `[USERNAME]@*example*.com`
- **Patrón de nombre de inicio de sesión de nivel inferior (Active Directory y Azure)**: `*example*\[USERNAME]`
- **Patrón de nombre distinguido**: `CN=[USERNAME],CN=Users,DC=*example*,DC=com`

  Incluya **[NOMBRE DE USUARIO]** exactamente como está escrito.

6. En la sección Seguridad de la capa de transporte (TLS), seleccione una configuración de seguridad.
   ◦ **Usar STARTTLS**: utilice STARTTLS para proteger las comunicaciones con el servidor LDAP. Esta es la opción recomendada para Active Directory, OpenLDAP u otros, pero esta opción no es compatible con Azure.
   ◦ **Usar LDAPS**: La opción LDAPS (LDAP sobre SSL) utiliza TLS para establecer una conexión con el servidor LDAP. Debe seleccionar esta opción para Azure.
   ◦ **No utilizar TLS**: El tráfico de red entre el sistema StorageGRID y el servidor LDAP no estará protegido. Esta opción no es compatible con Azure.

No se admite el uso de la opción **No usar TLS** si su servidor de Active Directory aplica la firma LDAP. Debe utilizar STARTTLS o LDAPS.

7. Si seleccionó STARTTLS o LDAPS, elija el certificado utilizado para proteger la conexión.
   - **Usar certificado CA del sistema operativo**: utilice el certificado CA de Grid predeterminado instalado en el sistema operativo para proteger las conexiones.
   - **Usar certificado CA personalizado**: utilice un certificado de seguridad personalizado.

     Si selecciona esta configuración, copie y pegue el certificado de seguridad personalizado en el cuadro de texto del certificado de CA.

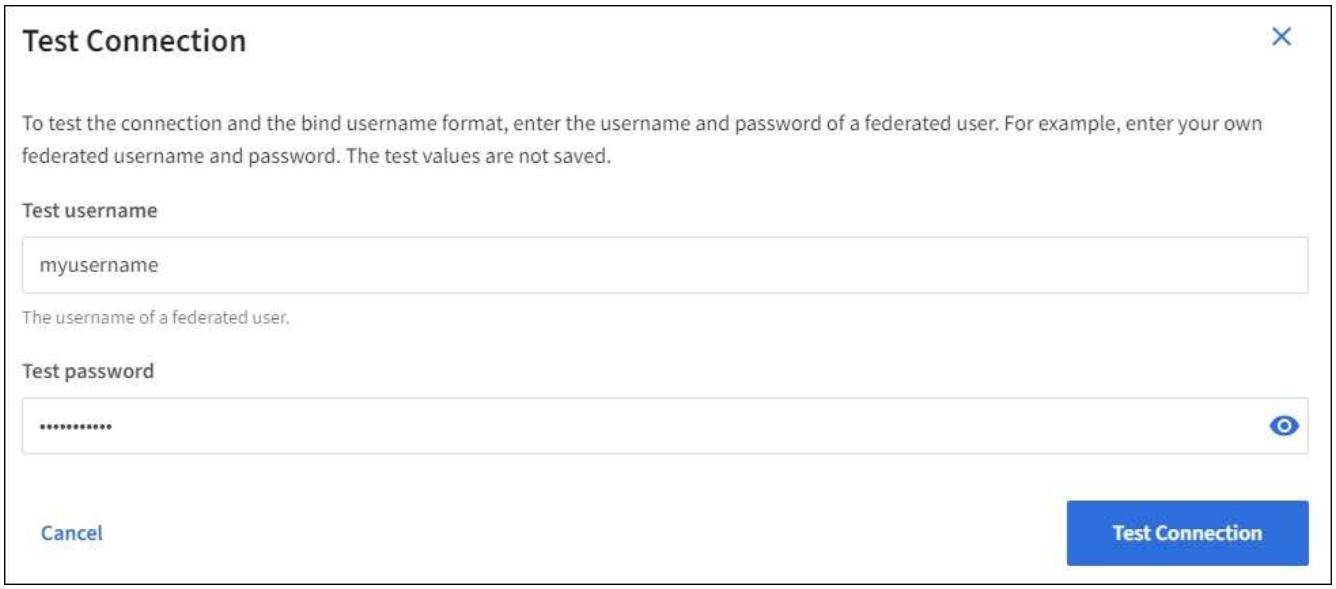
Pruebe la conexión y guarde la configuración

Después de ingresar todos los valores, debe probar la conexión antes de poder guardar la configuración. StorageGRID verifica la configuración de conexión para el servidor LDAP y el formato de nombre de usuario vinculado, si proporcionó uno.

Pasos

1. Seleccione **Probar conexión**.
2. Si no proporcionó un formato de nombre de usuario vinculado:
   - Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.
   - Aparece el mensaje "No se pudo establecer la conexión de prueba" si la configuración de conexión no es válida. Seleccione **Cerrar**. Luego, resuelva cualquier problema y pruebe la conexión nuevamente.
3. Si proporcionó un formato de nombre de usuario vinculado, ingrese el nombre de usuario y la contraseña de un usuario federado válido.

   Por ejemplo, ingrese su propio nombre de usuario y contraseña. No incluya ningún carácter especial en el nombre de usuario, como @ o /.



   - Aparecerá el mensaje "Conexión de prueba exitosa" si la configuración de conexión es válida. Seleccione **Guardar** para guardar la configuración.

- Aparece un mensaje de error si la configuración de conexión, el formato de nombre de usuario vinculado o el nombre de usuario y la contraseña de prueba no son válidos. Resuelva cualquier problema y pruebe la conexión nuevamente.

Forzar la sincronización con la fuente de identidad

El sistema StorageGRID sincroniza periódicamente los grupos y usuarios federados desde la fuente de identidad. Puede forzar el inicio de la sincronización si desea habilitar o restringir los permisos de usuario lo más rápido posible.

Pasos

1. Vaya a la página de federación de identidad.
2. Seleccione **Servidor de sincronización** en la parte superior de la página.

   El proceso de sincronización puede tardar algún tiempo dependiendo de su entorno.

> La alerta **Error de sincronización de federación de identidad** se activa si hay un problema al sincronizar grupos y usuarios federados desde la fuente de identidad.

Deshabilitar la federación de identidades

Puede deshabilitar temporal o permanentemente la federación de identidad para grupos y usuarios. Cuando la federación de identidad está deshabilitada, no hay comunicación entre StorageGRID y la fuente de identidad. Sin embargo, cualquier configuración que haya realizado se conservará, lo que le permitirá volver a habilitar fácilmente la federación de identidad en el futuro.

Acerca de esta tarea

Antes de deshabilitar la federación de identidad, debe tener en cuenta lo siguiente:

- Los usuarios federados no podrán iniciar sesión.
- Los usuarios federados que actualmente hayan iniciado sesión conservarán el acceso al sistema StorageGRID hasta que su sesión expire, pero no podrán iniciar sesión una vez que expire su sesión.
- No se producirá sincronización entre el sistema StorageGRID y la fuente de identidad, y no se generarán alertas para las cuentas que no se hayan sincronizado.
- La casilla de verificación **Habilitar federación de identidad** está deshabilitada si el inicio de sesión único (SSO) está configurado en **Habilitado** o **Modo Sandbox**. El estado de SSO en la página de inicio de sesión único debe ser **Deshabilitado** antes de poder deshabilitar la federación de identidad. Ver "Deshabilitar el inicio de sesión único" .

Pasos

1. Vaya a la página de federación de identidad.
2. Desmarque la casilla de verificación **Habilitar federación de identidad**.

Directrices para configurar un servidor OpenLDAP

Si desea utilizar un servidor OpenLDAP para la federación de identidad, debe configurar ajustes específicos en el servidor OpenLDAP.

Para las fuentes de identidad que no sean ActiveDirectory o Azure, StorageGRID no bloqueará automáticamente el acceso a S3 a los usuarios que estén deshabilitados externamente. Para bloquear el acceso a S3, elimine todas las claves S3 del usuario o elimine el usuario de todos los grupos.

Superposiciones de miembros y refinaciones

Las superposiciones memberof y refint deben estar habilitadas. Para obtener más información, consulte las instrucciones para el mantenimiento inverso de la membresía del grupo enhttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^] .

Indexación

Debe configurar los siguientes atributos OpenLDAP con las palabras clave de índice especificadas:

- `olcDbIndex: objectClass eq`
- `olcDbIndex: uid eq,pres,sub`
- `olcDbIndex: cn eq,pres,sub`
- `olcDbIndex: entryUUID eq`

Además, asegúrese de que los campos mencionados en la ayuda para el nombre de usuario estén indexados para un rendimiento óptimo.

Consulte la información sobre el mantenimiento de la membresía del grupo inverso en elhttp://www.openldap.org/doc/admin24/index.html["Documentación de OpenLDAP: Guía del administrador de la versión 2.4"^] .

Administrar grupos de administradores

Puede crear grupos de administradores para administrar los permisos de seguridad de uno o más usuarios administradores. Los usuarios deben pertenecer a un grupo para tener acceso al sistema StorageGRID .

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Si planea importar un grupo federado, ha configurado la federación de identidad y el grupo federado ya existe en la fuente de identidad configurada.

Crear un grupo de administradores

Los grupos de administradores le permiten determinar qué usuarios pueden acceder a qué funciones y operaciones en el Administrador de Grid y la API de administración de Grid.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Grupos de administradores**.

2. Seleccione **Crear grupo**.

Elija un tipo de grupo

Puede crear un grupo local o importar un grupo federado.

- Cree un grupo local si desea asignar permisos a usuarios locales.
- Cree un grupo federado para importar usuarios desde la fuente de identidad.

Grupo local

Pasos

1. Seleccione **Grupo local**.
2. Introduzca un nombre para mostrar para el grupo, que podrá actualizar más tarde según sea necesario. Por ejemplo, "Usuarios de mantenimiento" o "Administradores de ILM".
3. Introduzca un nombre único para el grupo, que no podrá actualizar más tarde.
4. Seleccione **Continuar**.

Grupo federado

Pasos

1. Seleccione **Grupo federado**.
2. Ingrese el nombre del grupo que desea importar, exactamente como aparece en la fuente de identidad configurada.
   - Para Active Directory y Azure, utilice sAMAccountName.
   - Para OpenLDAP, utilice el CN (nombre común).
   - Para otro LDAP, utilice el nombre único apropiado para el servidor LDAP.
3. Seleccione **Continuar**.

Administrar permisos de grupo

Pasos

1. Para **Modo de acceso**, seleccione si los usuarios del grupo pueden cambiar configuraciones y realizar operaciones en el Administrador de cuadrícula y la API de administración de cuadrícula o si solo pueden ver configuraciones y funciones.
   - **Lectura y escritura** (predeterminado): los usuarios pueden cambiar la configuración y realizar las operaciones permitidas por sus permisos de administración.
   - **Solo lectura**: los usuarios solo pueden ver configuraciones y funciones. No pueden realizar ningún cambio ni realizar ninguna operación en el Administrador de Grid ni en la API de administración de Grid. Los usuarios locales de solo lectura pueden cambiar sus propias contraseñas.

     Si un usuario pertenece a varios grupos y alguno de ellos está configurado como **Solo lectura**, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

2. Seleccione uno o más"permisos del grupo de administradores" .

   Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenecen al grupo no

podrán iniciar sesión en StorageGRID.

3. Si está creando un grupo local, seleccione **Continuar**. Si está creando un grupo federado, seleccione **Crear grupo** y **Finalizar**.

Agregar usuarios (solo grupos locales)

Pasos

1. Opcionalmente, seleccione uno o más usuarios locales para este grupo.

   Si aún no ha creado usuarios locales, puede guardar el grupo sin agregar usuarios. Puede agregar este grupo al usuario en la página Usuarios. Ver"Administrar usuarios" Para más detalles.

2. Seleccione **Crear grupo** y **Finalizar**.

Ver y editar grupos de administradores

Puede ver detalles de grupos existentes, modificar un grupo o duplicar un grupo.

- Para ver información básica de todos los grupos, revise la tabla en la página Grupos.
- Para ver todos los detalles de un grupo específico o editar un grupo, utilice el menú **Acciones** o la página de detalles.

Tarea	Menú de acciones	Página de detalles
Ver detalles del grupo	a. Seleccione la casilla de verificación del grupo. b. Seleccione **Acciones** > **Ver detalles del grupo**.	Seleccione el nombre del grupo en la tabla.
Editar nombre para mostrar (solo grupos locales)	a. Seleccione la casilla de verificación del grupo. b. Seleccione **Acciones** > **Editar nombre del grupo**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del grupo para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.
Editar el modo de acceso o los permisos	a. Seleccione la casilla de verificación del grupo. b. Seleccione **Acciones** > **Ver detalles del grupo**. c. Opcionalmente, cambie el modo de acceso del grupo. d. Opcionalmente, seleccione o desmarque"permisos del grupo de administradores" . e. Seleccione **Guardar cambios**.	a. Seleccione el nombre del grupo para mostrar los detalles. b. Opcionalmente, cambie el modo de acceso del grupo. c. Opcionalmente, seleccione o desmarque"permisos del grupo de administradores" . d. Seleccione **Guardar cambios**.

Duplicar un grupo

Pasos

1. Seleccione la casilla de verificación del grupo.
2. Seleccione **Acciones** > **Duplicar grupo**.
3. Complete el asistente para duplicar grupo.

Eliminar un grupo

Puede eliminar un grupo de administradores cuando desee eliminar el grupo del sistema y eliminar todos los permisos asociados con el grupo. Al eliminar un grupo de administradores se eliminan todos los usuarios del grupo, pero no se eliminan los usuarios mismos.

Pasos

1. Desde la página Grupos, seleccione la casilla de verificación de cada grupo que desee eliminar.
2. Seleccione **Acciones** > **Eliminar grupo**.
3. Seleccione **Eliminar grupos**.

Permisos del grupo de administradores

Al crear grupos de usuarios administradores, selecciona uno o más permisos para controlar el acceso a funciones específicas del Administrador de cuadrícula. Luego puede asignar cada usuario a uno o más de estos grupos de administración para determinar qué tareas puede realizar ese usuario.

Debe asignar al menos un permiso a cada grupo; de lo contrario, los usuarios que pertenecen a ese grupo no podrán iniciar sesión en Grid Manager ni en la API de administración de Grid.

De forma predeterminada, cualquier usuario que pertenezca a un grupo que tenga al menos un permiso puede realizar las siguientes tareas:

- Sign in en el Administrador de cuadrícula
- Ver el panel de control
- Ver las páginas de Nodos
- Ver alertas actuales y resueltas
- Cambiar su propia contraseña (sólo usuarios locales)
- Ver cierta información proporcionada en las páginas de Configuración y Mantenimiento

Interacción entre permisos y modo de acceso

Para todos los permisos, la configuración **Modo de acceso** del grupo determina si los usuarios pueden cambiar configuraciones y realizar operaciones o si solo pueden ver las configuraciones y funciones relacionadas. Si un usuario pertenece a varios grupos y alguno de ellos está configurado como **Solo lectura**, el usuario tendrá acceso de solo lectura a todas las configuraciones y funciones seleccionadas.

Las siguientes secciones describen los permisos que puede asignar al crear o editar un grupo de administradores. Cualquier funcionalidad no mencionada explícitamente requiere el permiso de **acceso root**.

Acceso root

Este permiso proporciona acceso a todas las funciones de administración de la red.

Cambiar la contraseña raíz del inquilino

Este permiso proporciona acceso a la opción **Cambiar contraseña root** en la página Inquilinos, lo que le permite controlar quién puede cambiar la contraseña del usuario root local del inquilino. Este permiso también se utiliza para migrar claves S3 cuando la función de importación de claves S3 está habilitada. Los usuarios que no tienen este permiso no pueden ver la opción **Cambiar contraseña root**.

> Para otorgar acceso a la página Inquilinos, que contiene la opción **Cambiar contraseña root**, asigne también el permiso **Cuentas de inquilinos**.

Configuración de la página de topología de cuadrícula

Este permiso proporciona acceso a las pestañas de Configuración en la página **SOPORTE** > **Herramientas** > **Topología de cuadrícula**.

> La página de topología de cuadrícula ha quedado obsoleta y se eliminará en una versión futura.

ILM

Este permiso proporciona acceso a las siguientes opciones del menú **ILM**:

- Normas
- Políticas
- Etiquetas de política
- Pools de almacenamiento
- Grados de almacenamiento
- Regiones
- Búsqueda de metadatos de objetos

> Los usuarios deben tener los permisos **Otra configuración de red** y **Configuración de página de topología de red** para administrar los niveles de almacenamiento.

Mantenimiento

Los usuarios deben tener el permiso de Mantenimiento para utilizar estas opciones:

- **CONFIGURACIÓN** > **Control de acceso**:
  - Contraseñas de la red
- **CONFIGURACIÓN** > **Red**:
  - Nombres de dominio de punto final S3
- **MANTENIMIENTO** > **Tareas**:
  - Desmantelamiento

    - Expansión
    - Comprobación de existencia de objetos
    - Recuperación
- **MANTENIMIENTO** > **Sistema**:
    - Paquete de recuperación
    - Actualización de software
- **SOPORTE** > **Herramientas**:
    - Registros

Los usuarios que no tienen el permiso de Mantenimiento pueden ver, pero no editar, estas páginas:

- **MANTENIMIENTO** > **Red**:
    - servidores DNS
    - Red de cuadrícula
    - servidores NTP
- **MANTENIMIENTO** > **Sistema**:
    - Licencia
- **CONFIGURACIÓN** > **Red**:
    - Nombres de dominio de punto final S3
- **CONFIGURACIÓN** > **Seguridad**:
    - Certificados
- **CONFIGURACIÓN** > **Monitoreo**:
    - Servidor de auditoría y syslog

Administrar alertas

Este permiso proporciona acceso a opciones para administrar alertas. Los usuarios deben tener este permiso para administrar silencios, notificaciones de alerta y reglas de alerta.

Consulta de métricas

Este permiso proporciona acceso a:

- **SOPORTE** > **Herramientas** > Página **Métricas**
- Consultas de métricas de Prometheus personalizadas mediante la sección **Métricas** de la API de administración de cuadrícula
- Tarjetas del panel de control de Grid Manager que contienen métricas

Búsqueda de metadatos de objetos

Este permiso proporciona acceso a la página **ILM** > **Búsqueda de metadatos de objetos**.

Otra configuración de red

Este permiso proporciona acceso a opciones de configuración de cuadrícula adicionales.

> Para ver estas opciones adicionales, los usuarios también deben tener el permiso **Configuración de la página de topología de cuadrícula**.

- **ILM**:
  - Grados de almacenamiento
- **CONFIGURACIÓN** > **Sistema**:
- **SOPORTE** > **Otro**:
  - Costo del enlace

Administrador de dispositivos de almacenamiento

Este permiso proporciona:

- Acceso al E-Series SANtricity System Manager en dispositivos de almacenamiento a través del Grid Manager.
- La capacidad de realizar tareas de resolución de problemas y mantenimiento en la pestaña Administrar unidades para dispositivos que admiten estas operaciones.

Cuentas de inquilinos

Este permiso proporciona la capacidad de:

- Acceda a la página Inquilinos, donde puede crear, editar y eliminar cuentas de inquilinos
- Ver las políticas de clasificación de tráfico existentes
- Ver las tarjetas del panel de Grid Manager que contienen detalles de los inquilinos

Administrar usuarios

Puede ver usuarios locales y federados. También puede crear usuarios locales y asignarlos a grupos de administradores locales para determinar a qué funciones de Grid Manager pueden acceder estos usuarios.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .

Crear un usuario local

Puede crear uno o más usuarios locales y asignar cada usuario a uno o más grupos locales. Los permisos del grupo controlan a qué funciones de Grid Manager y Grid Management API puede acceder el usuario.

Sólo puedes crear usuarios locales. Utilice la fuente de identidad externa para administrar usuarios y grupos federados.

El administrador de cuadrícula incluye un usuario local predefinido, llamado "root". No puedes eliminar el usuario root.

> Si el inicio de sesión único (SSO) está habilitado, los usuarios locales no pueden iniciar sesión en StorageGRID.

Acceder al asistente

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Usuarios administradores**.
2. Seleccione **Crear usuario**.

Ingrese las credenciales de usuario

Pasos

1. Introduzca el nombre completo del usuario, un nombre de usuario único y una contraseña.
2. Opcionalmente, seleccione **Sí** si este usuario no debe tener acceso al Administrador de Grid o a la API de administración de Grid.
3. Seleccione **Continuar**.

Asignar a grupos

Pasos

1. Opcionalmente, asigne el usuario a uno o más grupos para determinar los permisos del usuario.

   Si aún no ha creado grupos, puede guardar el usuario sin seleccionar grupos. Puede agregar este usuario a un grupo en la página Grupos.

   Si un usuario pertenece a varios grupos, los permisos son acumulativos. Ver"Administrar grupos de administradores" Para más detalles.

2. Seleccione **Crear usuario** y seleccione **Finalizar**.

Ver y editar usuarios locales

Puede ver detalles de los usuarios locales y federados existentes. Puede modificar un usuario local para cambiar su nombre completo, contraseña o membresía de grupo. También puede impedir temporalmente que un usuario acceda al Administrador de Grid y a la API de administración de Grid.

Sólo puedes editar usuarios locales. Utilice la fuente de identidad externa para administrar usuarios federados.

- Para ver información básica de todos los usuarios locales y federados, revise la tabla en la página Usuarios.
- Para ver todos los detalles de un usuario específico, editar un usuario local o cambiar la contraseña de un usuario local, utilice el menú **Acciones** o la página de detalles.

  Cualquier edición se aplicará la próxima vez que el usuario cierre sesión y vuelva a iniciar sesión en el Administrador de cuadrícula.

> Los usuarios locales pueden cambiar sus propias contraseñas utilizando la opción **Cambiar contraseña** en el banner de Grid Manager.

Tarea	Menú de acciones	Página de detalles
Ver detalles del usuario	a. Seleccione la casilla de verificación para el usuario. b. Seleccione **Acciones** > **Ver detalles del usuario**.	Seleccione el nombre del usuario en la tabla.
Editar nombre completo (solo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione **Acciones** > **Editar nombre completo**. c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione el icono de edición . c. Introduzca el nuevo nombre. d. Seleccione **Guardar cambios**.
Denegar o permitir el acceso a StorageGRID	a. Seleccione la casilla de verificación para el usuario. b. Seleccione **Acciones** > **Ver detalles del usuario**. c. Seleccione la pestaña Acceso. d. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de administración de Grid, o seleccione **No** para permitir que el usuario inicie sesión. e. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Acceso. c. Seleccione **Sí** para evitar que el usuario inicie sesión en Grid Manager o en la API de administración de Grid, o seleccione **No** para permitir que el usuario inicie sesión. d. Seleccione **Guardar cambios**.
Cambiar contraseña (sólo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione **Acciones** > **Ver detalles del usuario**. c. Seleccione la pestaña Contraseña. d. Introduzca una nueva contraseña. e. Seleccione **Cambiar contraseña**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Contraseña. c. Introduzca una nueva contraseña. d. Seleccione **Cambiar contraseña**.

Tarea	Menú de acciones	Página de detalles
Cambiar grupos (solo usuarios locales)	a. Seleccione la casilla de verificación para el usuario. b. Seleccione **Acciones** > **Ver detalles del usuario**. c. Seleccione la pestaña Grupos. d. Opcionalmente, seleccione el enlace después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. e. Seleccione **Editar grupos** para seleccionar diferentes grupos. f. Seleccione **Guardar cambios**.	a. Seleccione el nombre del usuario para mostrar los detalles. b. Seleccione la pestaña Grupos. c. Opcionalmente, seleccione el enlace después del nombre de un grupo para ver los detalles del grupo en una nueva pestaña del navegador. d. Seleccione **Editar grupos** para seleccionar diferentes grupos. e. Seleccione **Guardar cambios**.

Duplicar un usuario

Puede duplicar un usuario existente para crear un nuevo usuario con los mismos permisos.

Pasos

1. Seleccione la casilla de verificación para el usuario.
2. Seleccione **Acciones** > **Duplicar usuario**.
3. Complete el asistente para duplicar usuarios.

Eliminar un usuario

Puede eliminar un usuario local para eliminarlo permanentemente del sistema.

No puedes eliminar el usuario root.

Pasos

1. Desde la página Usuarios, seleccione la casilla de verificación de cada usuario que desee eliminar.
2. Seleccione **Acciones** > **Eliminar usuario**.
3. Seleccione **Eliminar usuario**.

Utilice el inicio de sesión único (SSO)

Configurar el inicio de sesión único

Cuando el inicio de sesión único (SSO) está habilitado, los usuarios solo pueden acceder a Grid Manager, Tenant Manager, Grid Management API o Tenant Management API si sus credenciales están autorizadas mediante el proceso de inicio de sesión SSO implementado por su organización. Los usuarios locales no pueden iniciar sesión en StorageGRID.

Cómo funciona el inicio de sesión único

El sistema StorageGRID admite el inicio de sesión único (SSO) mediante el estándar Security Assertion Markup Language 2.0 (SAML 2.0).

Antes de habilitar el inicio de sesión único (SSO), revise cómo se ven afectados los procesos de inicio y cierre de sesión de StorageGRID cuando se habilita el SSO.

Sign in cuando el SSO esté habilitado

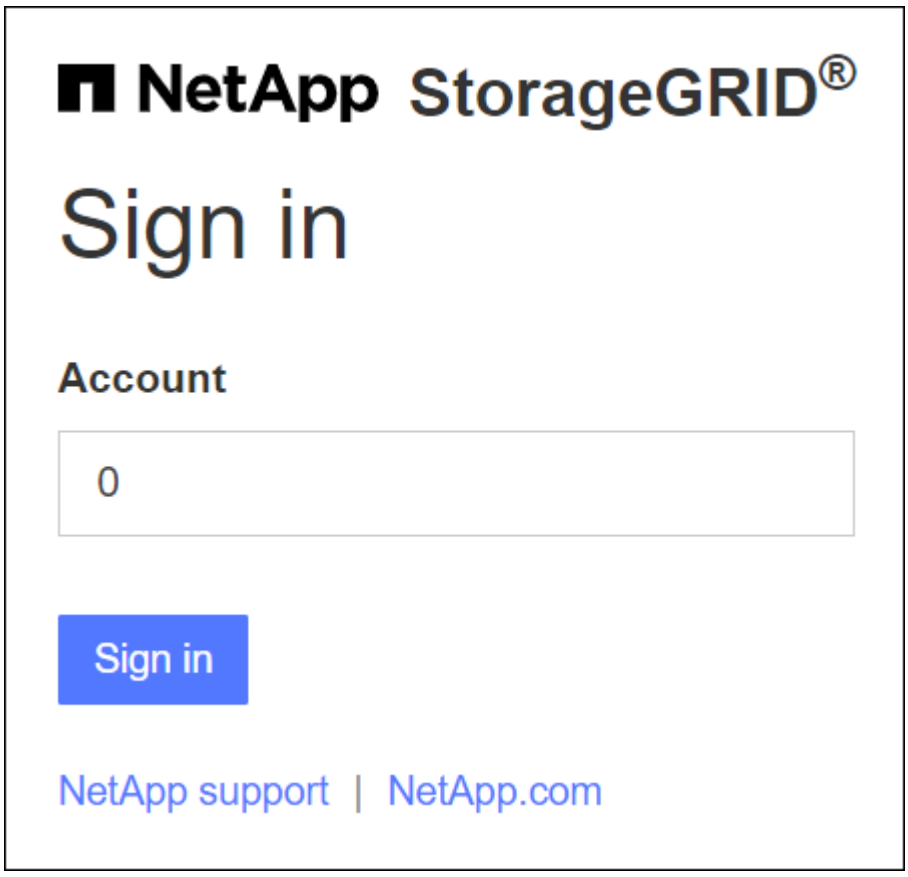
Cuando SSO está habilitado e inicia sesión en StorageGRID, se lo redirige a la página SSO de su organización para validar sus credenciales.

Pasos

1. Ingrese el nombre de dominio completo o la dirección IP de cualquier nodo de administración de StorageGRID en un navegador web.

   Aparece la página de Sign in de StorageGRID .

   - Si es la primera vez que accede a la URL en este navegador, se le solicitará un ID de cuenta:

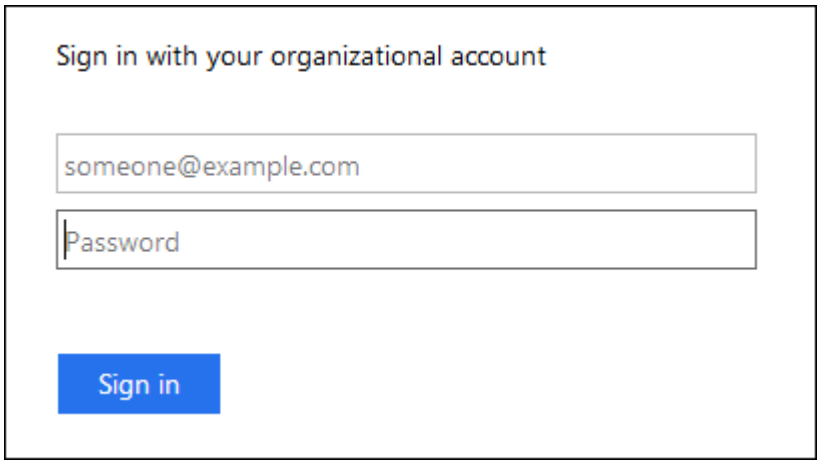


   - Si ya ha accedido al Administrador de red o al Administrador de inquilinos, se le solicitará que seleccione una cuenta reciente o que ingrese un ID de cuenta:

La página de Sign in de StorageGRID no se muestra cuando ingresa la URL completa para una cuenta de inquilino (es decir, un nombre de dominio completo o una dirección IP seguida de `/?accountId=20-digit-account-id`). En su lugar, se le redirige inmediatamente a la página de inicio de sesión SSO de su organización, donde puedeInicie sesión con sus credenciales de SSO .

2. Indique si desea acceder al Administrador de red o al Administrador de inquilinos:
   - Para acceder al Administrador de cuadrícula, deje el campo **ID de cuenta** en blanco, ingrese **0** como ID de cuenta o seleccione **Administrador de cuadrícula** si aparece en la lista de cuentas recientes.
   - Para acceder al Administrador de inquilinos, ingrese el ID de la cuenta del inquilino de 20 dígitos o seleccione un inquilino por nombre si aparece en la lista de cuentas recientes.
3. Seleccionar * Sign in*

   StorageGRID lo redirecciona a la página de inicio de sesión SSO de su organización. Por ejemplo:



4. Sign in con sus credenciales SSO.

Si sus credenciales de SSO son correctas:

a. El proveedor de identidad (IdP) proporciona una respuesta de autenticación a StorageGRID.
b. StorageGRID valida la respuesta de autenticación.
c. Si la respuesta es válida y usted pertenece a un grupo federado con permisos de acceso a StorageGRID , iniciará sesión en Grid Manager o en Tenant Manager, según la cuenta que haya seleccionado.

> Si la cuenta de servicio no es accesible, aún puede iniciar sesión, siempre que sea un usuario existente que pertenezca a un grupo federado con permisos de acceso a StorageGRID .

5. Opcionalmente, acceda a otros nodos de administración, o acceda al Administrador de red o al Administrador de inquilinos, si tiene los permisos adecuados.

   No es necesario volver a ingresar sus credenciales SSO.

Cerrar sesión cuando el SSO esté habilitado

Cuando SSO está habilitado para StorageGRID, lo que sucede cuando cierra sesión depende de dónde haya iniciado sesión y desde dónde cierre sesión.

Pasos

1. Localice el enlace **Cerrar sesión** en la esquina superior derecha de la interfaz de usuario.
2. Seleccione **Cerrar sesión**.

   Aparece la página de Sign in de StorageGRID . El menú desplegable **Cuentas recientes** se actualiza para incluir **Grid Manager** o el nombre del inquilino, para que pueda acceder a estas interfaces de usuario más rápidamente en el futuro.

Si ha iniciado sesión en…	Y cierras sesión en…	Has cerrado sesión en…
Administrador de cuadrícula en uno o más nodos de administración	Administrador de cuadrícula en cualquier nodo de administración	Administrador de cuadrícula en todos los nodos de administración **Nota:** Si usa Azure para SSO, puede que lleve algunos minutos cerrar sesión en todos los nodos de administración.
Administrador de inquilinos en uno o más nodos de administración	Administrador de inquilinos en cualquier nodo de administración	Administrador de inquilinos en todos los nodos de administración
Tanto Grid Manager como Tenant Manager	Administrador de red	Sólo el administrador de cuadrícula. También debe cerrar sesión en el Administrador de inquilinos para cerrar sesión en SSO.

La tabla resume lo que sucede cuando cierras sesión si estás usando una sola sesión de navegador. Si ha iniciado sesión en StorageGRID en varias sesiones de navegador, deberá cerrar sesión en todas las sesiones de navegador por separado.

Requisitos y consideraciones para el inicio de sesión único

Antes de habilitar el inicio de sesión único (SSO) para un sistema StorageGRID , revise los requisitos y las consideraciones.

Requisitos del proveedor de identidad

StorageGRID admite los siguientes proveedores de identidad SSO (IdP):

- Servicio de federación de Active Directory (AD FS)
- Directorio activo de Azure (Azure AD)
- Federación de ping

Debe configurar la federación de identidad para su sistema StorageGRID antes de poder configurar un proveedor de identidad SSO. El tipo de servicio LDAP que utiliza para la federación de identidad controla qué tipo de SSO puede implementar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Requisitos de AD FS

Puede utilizar cualquiera de las siguientes versiones de AD FS:

- ADFS de Windows Server 2022
- Servidor AD FS de Windows 2019
- Servidor AD FS de Windows 2016

Windows Server 2016 debería utilizar el "Actualización KB3201845" , o superior.

Requisitos adicionales

- Seguridad de la capa de transporte (TLS) 1.2 o 1.3
- Microsoft .NET Framework, versión 3.5.1 o superior

Consideraciones para Azure

Si usa Azure como tipo de SSO y los usuarios tienen nombres principales de usuario que no usan sAMAccountName como prefijo, pueden surgir problemas de inicio de sesión si StorageGRID pierde su

conexión con el servidor LDAP. Para permitir que los usuarios inicien sesión, debe restaurar la conexión al servidor LDAP.

Requisitos del certificado de servidor

De forma predeterminada, StorageGRID utiliza un certificado de interfaz de administración en cada nodo de administración para proteger el acceso al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Cuando configura relaciones de confianza de usuario confiable (AD FS), aplicaciones empresariales (Azure) o conexiones de proveedor de servicios (PingFederate) para StorageGRID, utiliza el certificado del servidor como certificado de firma para las solicitudes de StorageGRID .

Si aún no lo has hecho"Configuró un certificado personalizado para la interfaz de administración" Deberías hacerlo ahora. Cuando instala un certificado de servidor personalizado, este se utiliza para todos los nodos de administración y puede usarlo en todas las relaciones de confianza de usuarios confiables de StorageGRID , aplicaciones empresariales o conexiones de SP .

> ⓘ No se recomienda utilizar el certificado de servidor predeterminado de un nodo de administración en una relación de confianza de usuario confiable, una aplicación empresarial o una conexión de SP . Si el nodo falla y lo recupera, se genera un nuevo certificado de servidor predeterminado. Antes de poder iniciar sesión en el nodo recuperado, debe actualizar la confianza de la parte confiable, la aplicación empresarial o la conexión del SP con el nuevo certificado.

Puede acceder al certificado de servidor de un nodo de administración iniciando sesión en el shell de comandos del nodo y yendo a `/var/local/mgmt-api` directorio. Un certificado de servidor personalizado se denomina `custom-server.crt` . El certificado de servidor predeterminado del nodo se llama `server.crt` .

Requisitos del puerto

El inicio de sesión único (SSO) no está disponible en los puertos restringidos de Grid Manager o Tenant Manager. Debe utilizar el puerto HTTPS predeterminado (443) si desea que los usuarios se autentiquen con inicio de sesión único. Ver "Controlar el acceso al firewall externo" .

Confirmar que los usuarios federados puedan iniciar sesión

Antes de habilitar el inicio de sesión único (SSO), debe confirmar que al menos un usuario federado pueda iniciar sesión en Grid Manager y en Tenant Manager para cualquier cuenta de inquilino existente.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .
- Ya ha configurado la federación de identidad.

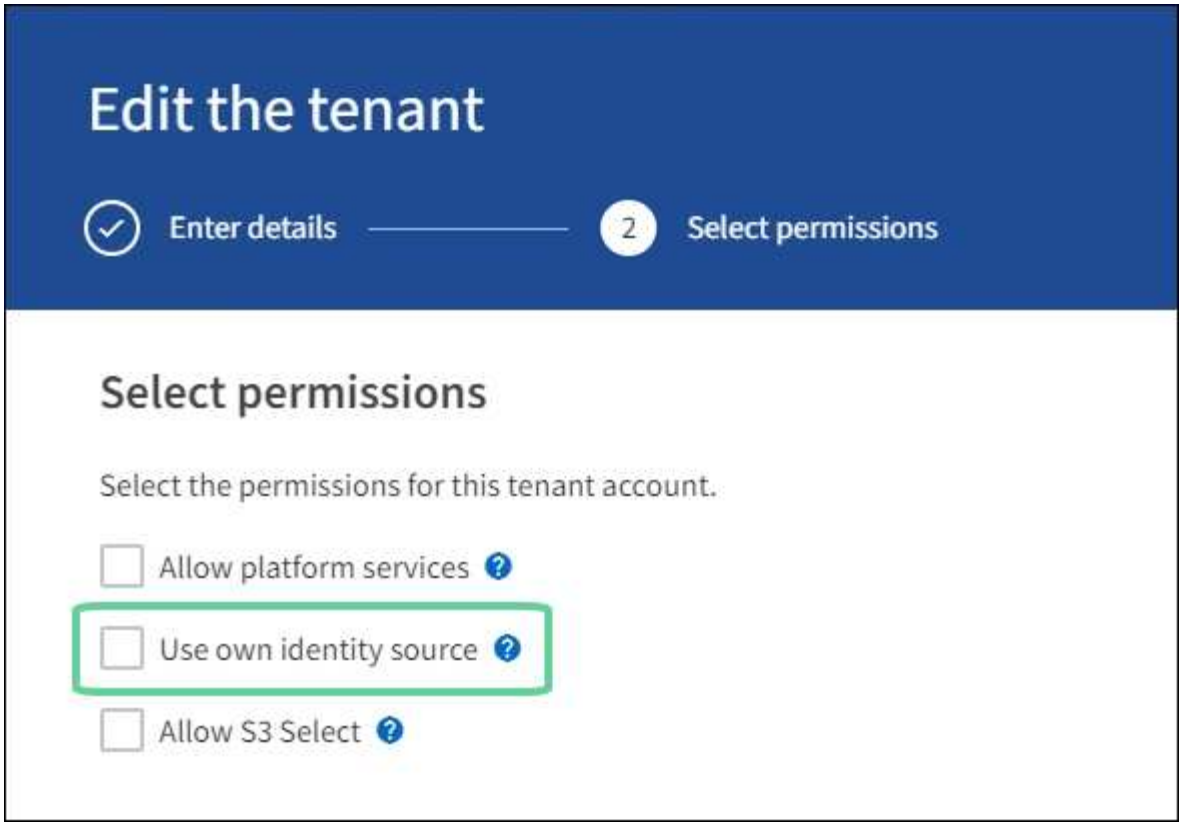
Pasos

1. Si existen cuentas de inquilinos, confirme que ninguno de ellos esté usando su propia fuente de identidad.

Cuando habilita SSO, una fuente de identidad configurada en Tenant Manager se reemplaza por la fuente de identidad configurada en Grid Manager. Los usuarios que pertenecen a la fuente de identidad del inquilino ya no podrán iniciar sesión a menos que tengan una cuenta con la fuente de identidad de Grid Manager.

a. Sign in en el Administrador de inquilinos para cada cuenta de inquilino.
b. Seleccione **GESTIÓN DE ACCESO** > **Federación de identidades**.
c. Confirme que la casilla de verificación **Habilitar federación de identidad** no esté seleccionada.
d. Si es así, confirme que cualquier grupo federado que pueda estar en uso para esta cuenta de inquilino ya no sea necesario, desmarque la casilla de verificación y seleccione **Guardar**.

2. Confirme que un usuario federado puede acceder al Administrador de Grid:
   a. Desde Grid Manager, seleccione **CONFIGURACIÓN** > **Control de acceso** > **Grupos de administración**.
   b. Asegúrese de que se haya importado al menos un grupo federado desde la fuente de identidad de Active Directory y que se le haya asignado el permiso de acceso raíz.
   c. Desconectar.
   d. Confirme que puede volver a iniciar sesión en Grid Manager como usuario del grupo federado.
3. Si hay cuentas de inquilino existentes, confirme que un usuario federado que tenga permiso de acceso raíz pueda iniciar sesión:
   a. Desde el Administrador de red, seleccione **INQUILINOS**.
   b. Seleccione la cuenta del inquilino y seleccione **Acciones** > **Editar**.
   c. En la pestaña Ingresar detalles, seleccione **Continuar**.
   d. Si la casilla de verificación **Usar fuente de identidad propia** está seleccionada, desmarque la casilla y seleccione **Guardar**.



Aparece la página del inquilino.

a. Seleccione la cuenta del inquilino, seleccione * Sign in* e inicie sesión en la cuenta del inquilino como usuario raíz local.
b. Desde el Administrador de inquilinos, seleccione **ADMINISTRACIÓN DE ACCESO** > **Grupos**.
c. Asegúrese de que al menos a un grupo federado del Administrador de Grid se le haya asignado el permiso de acceso raíz para este inquilino.
d. Desconectar.
e. Confirme que puede volver a iniciar sesión en el inquilino como usuario en el grupo federado.

Información relacionada

- "Requisitos y consideraciones para el inicio de sesión único"
- "Administrar grupos de administradores"
- "Utilice una cuenta de inquilino"

Utilizar el modo sandbox

Puede utilizar el modo sandbox para configurar y probar el inicio de sesión único (SSO) antes de habilitarlo para todos los usuarios de StorageGRID . Una vez habilitado el SSO, puede regresar al modo sandbox siempre que necesite cambiar o volver a probar la configuración.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tú tienes el"Permiso de acceso root" .

- Ha configurado la federación de identidad para su sistema StorageGRID .
- Para la federación de identidad **tipo de servicio LDAP**, seleccionó Active Directory o Azure, según el proveedor de identidad SSO que planea usar.

Tipo de servicio LDAP configurado	Opciones para el proveedor de identidad SSO
Directorio activo	• Directorio activo • Azur • Federación de ping
Azur	Azur

Acerca de esta tarea

Cuando SSO está habilitado y un usuario intenta iniciar sesión en un nodo de administración, StorageGRID envía una solicitud de autenticación al proveedor de identidad SSO. A su vez, el proveedor de identidad SSO envía una respuesta de autenticación a StorageGRID, indicando si la solicitud de autenticación fue exitosa. Para solicitudes exitosas:

- La respuesta de Active Directory o PingFederate incluye un identificador único universal (UUID) para el usuario.
- La respuesta de Azure incluye un nombre principal de usuario (UPN).

Para permitir que StorageGRID (el proveedor de servicios) y el proveedor de identidad SSO se comuniquen de forma segura acerca de las solicitudes de autenticación de usuarios, debe configurar ciertas configuraciones en StorageGRID. A continuación, debe utilizar el software del proveedor de identidad SSO para crear una relación de confianza de usuario confiable (AD FS), una aplicación empresarial (Azure) o un proveedor de servicios (PingFederate) para cada nodo de administración. Por último, debes regresar a StorageGRID para habilitar SSO.

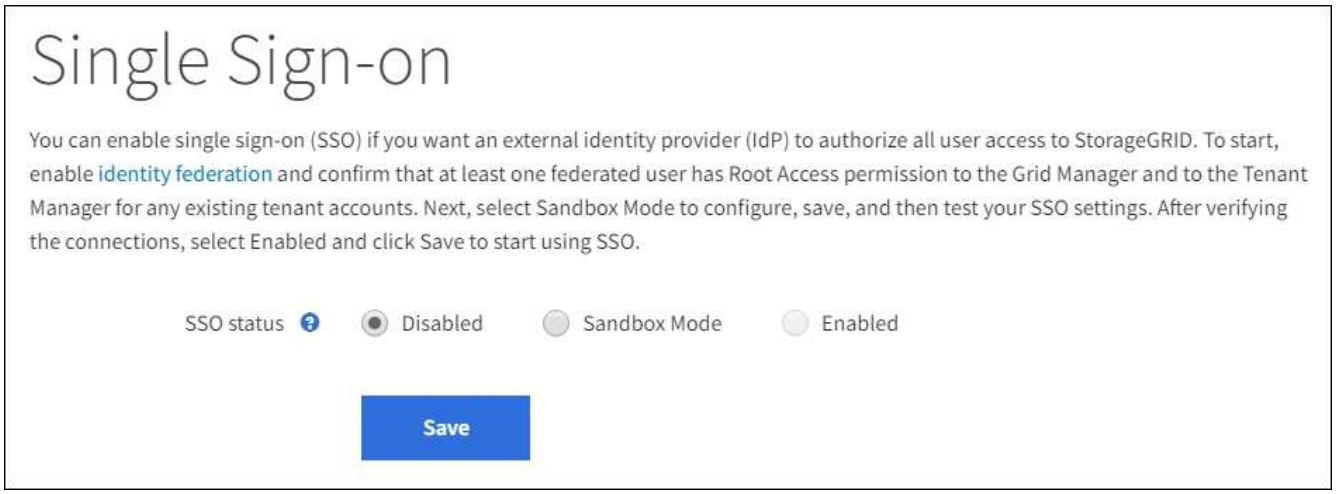
El modo Sandbox facilita la realización de esta configuración de ida y vuelta y permite probar todas las configuraciones antes de habilitar SSO. Cuando se utiliza el modo sandbox, los usuarios no pueden iniciar sesión mediante SSO.

Acceder al modo sandbox

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.

   Aparece la página de inicio de sesión único, con la opción **Deshabilitado** seleccionada.



Si las opciones de Estado de SSO no aparecen, confirme que haya configurado el proveedor de identidad como fuente de identidad federada. Ver "Requisitos y consideraciones para el inicio de sesión único" .

2. Seleccione **Modo Sandbox**.

   Aparece la sección Proveedor de identidad.

Introduzca los datos del proveedor de identidad

Pasos

1. Seleccione el **tipo de SSO** de la lista desplegable.
2. Complete los campos en la sección Proveedor de identidad según el tipo de SSO que haya seleccionado.

Directorio activo

a. Ingrese el **Nombre del servicio de federación** para el proveedor de identidad, exactamente como aparece en el Servicio de federación de Active Directory (AD FS).

> Para localizar el nombre del servicio de federación, vaya al Administrador de servidor de Windows. Seleccione **Herramientas** > **Administración de AD FS**. En el menú Acción, seleccione **Editar propiedades del servicio de federación**. El nombre del servicio de la federación se muestra en el segundo campo.

b. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

- **Usar certificado CA del sistema operativo**: utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado**: utilice un certificado CA personalizado para proteger la conexión.

  Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

- **No utilizar TLS**: No utilice un certificado TLS para proteger la conexión.

> Si cambia el certificado de CA, inmediatamente"reiniciar el servicio mgmt-api en los nodos de administración" y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

c. En la sección Parte confiada, especifique el **Identificador de parte confiada** para StorageGRID. Este valor controla el nombre que utiliza para cada relación de confianza de usuario confiable en AD FS.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese `SG` o `StorageGRID` .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Esto genera una tabla que muestra el identificador de la parte confiable para cada nodo de administración en su sistema, según el nombre de host del nodo.

> Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

d. Seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.

Azur

a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de StorageGRID .

   - **Usar certificado CA del sistema operativo**: utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
   - **Usar certificado CA personalizado**: utilice un certificado CA personalizado para proteger la conexión.

     Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

   - **No utilizar TLS**: No utilice un certificado TLS para proteger la conexión.

   > Si cambia el certificado de CA, inmediatamente"reiniciar el servicio mgmt-api en los nodos de administración" y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

b. En la sección Aplicación empresarial, especifique el **nombre de la aplicación empresarial** para StorageGRID. Este valor controla el nombre que utiliza para cada aplicación empresarial en Azure AD.

   - Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese `SG` o `StorageGRID` .
   - Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Esto genera una tabla que muestra un nombre de aplicación empresarial para cada nodo de administración en su sistema, según el nombre de host del nodo.

   > Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

c. Siga los pasos en"Crear aplicaciones empresariales en Azure AD" para crear una aplicación empresarial para cada nodo de administración enumerado en la tabla.

d. Desde Azure AD, copie la URL de metadatos de federación para cada aplicación empresarial. Luego, pegue esta URL en el campo **URL de metadatos de federación** correspondiente en StorageGRID.

e. Después de haber copiado y pegado una URL de metadatos de federación para todos los nodos de administración, seleccione **Guardar**.

   Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.

Federación de ping

a. Especifique qué certificado TLS se utilizará para proteger la conexión cuando el proveedor de identidad envíe información de configuración de SSO en respuesta a las solicitudes de

StorageGRID .

- **Usar certificado CA del sistema operativo**: utilice el certificado CA predeterminado instalado en el sistema operativo para proteger la conexión.
- **Usar certificado CA personalizado**: utilice un certificado CA personalizado para proteger la conexión.

  Si selecciona esta configuración, copie el texto del certificado personalizado y péguelo en el cuadro de texto **Certificado CA**.

- **No utilizar TLS**: No utilice un certificado TLS para proteger la conexión.

> Si cambia el certificado de CA, inmediatamente"reiniciar el servicio mgmt-api en los nodos de administración" y comprobar que el inicio de sesión único (SSO) en Grid Manager es exitoso.

b. En la sección Proveedor de servicios (SP), especifique el *ID de conexión de SP * para StorageGRID. Este valor controla el nombre que utiliza para cada conexión SP en PingFederate.

- Por ejemplo, si su red tiene solo un nodo de administración y no prevé agregar más nodos de administración en el futuro, ingrese `SG` o `StorageGRID` .
- Si su cuadrícula incluye más de un nodo de administración, incluya la cadena `[HOSTNAME]` en el identificador. Por ejemplo, `SG-[HOSTNAME]` . Esto genera una tabla que muestra el ID de conexión de SP para cada nodo de administración en su sistema, según el nombre de host del nodo.

> Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID . Tener una conexión SP para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

c. Especifique la URL de metadatos de la federación para cada nodo de administración en el campo **URL de metadatos de la federación**.

Utilice el siguiente formato:

```
https://<Federation Service
Name>:<port>/pf/federation_metadata.ping?PartnerSpId=<SP
Connection ID>
```

d. Seleccione **Guardar**.

Aparece una marca de verificación verde en el botón **Guardar** durante unos segundos.

Configurar relaciones de confianza entre usuarios, aplicaciones empresariales o conexiones de SP

Cuando se guarda la configuración, aparece el aviso de confirmación del modo Sandbox. Este aviso confirma que el modo sandbox ahora está habilitado y proporciona instrucciones generales.

StorageGRID puede permanecer en modo sandbox tanto tiempo como sea necesario. Sin embargo, cuando se selecciona **Modo Sandbox** en la página de Inicio de sesión único, el SSO se deshabilita para todos los usuarios de StorageGRID . Sólo los usuarios locales pueden iniciar sesión.

Siga estos pasos para configurar relaciones de confianza de usuarios autenticados (Active Directory), completar aplicaciones empresariales (Azure) o configurar conexiones de SP (PingFederate).

Directorio activo

Pasos

1. Vaya a Servicios de federación de Active Directory (AD FS).
2. Cree una o más relaciones de confianza de usuario confiable para StorageGRID, utilizando cada identificador de usuario confiable que se muestra en la tabla de la página de inicio de sesión único de StorageGRID .

   Debe crear una confianza para cada nodo de administración que se muestra en la tabla.

   Para obtener instrucciones, vaya a"Crear relaciones de confianza entre usuarios autenticados en AD FS" .

Azur

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
   a. Sign in en el nodo.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.
   c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya al Portal de Azure.
4. Siga los pasos en"Crear aplicaciones empresariales en Azure AD" para cargar el archivo de metadatos SAML para cada nodo de administración en su aplicación empresarial de Azure correspondiente.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único del nodo de administración en el que está conectado actualmente, seleccione el botón para descargar y guardar los metadatos SAML.
2. Luego, para cualquier otro nodo de administración en su red, repita estos pasos:
   a. Sign in en el nodo.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.
   c. Descargue y guarde los metadatos SAML para ese nodo.
3. Vaya a PingFederate.
4. "Cree una o más conexiones de proveedor de servicios (SP) para StorageGRID" . Utilice el ID de conexión de SP para cada nodo de administración (que se muestra en la tabla de la página de inicio de sesión único de StorageGRID) y los metadatos SAML que descargó para ese nodo de administración.

   Debe crear una conexión SP para cada nodo de administración que se muestra en la tabla.

Probar conexiones SSO

Antes de implementar el uso del inicio de sesión único para todo el sistema StorageGRID , debe confirmar que

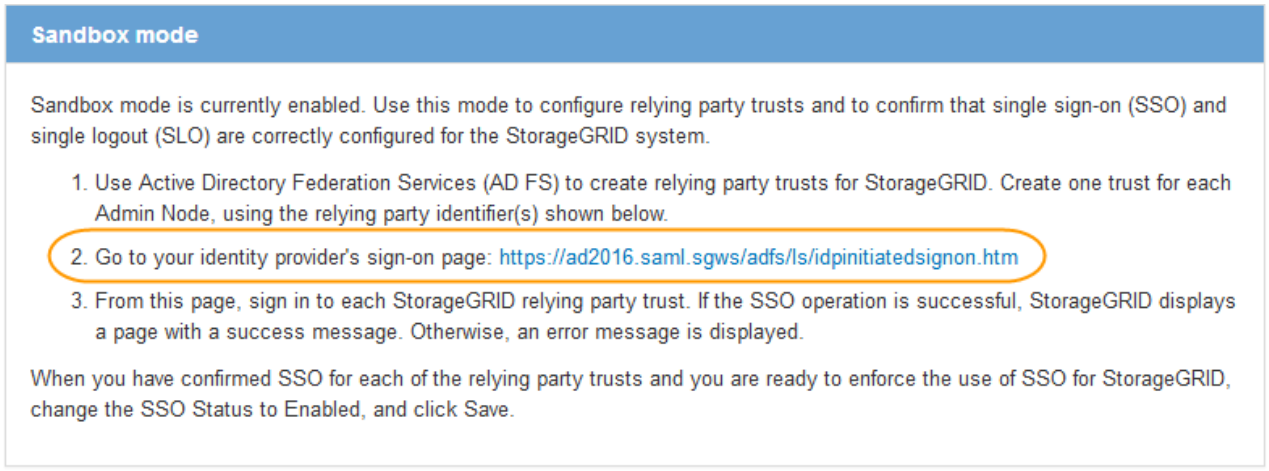
el inicio de sesión único y el cierre de sesión único estén configurados correctamente para cada nodo de administración.

Directorio activo

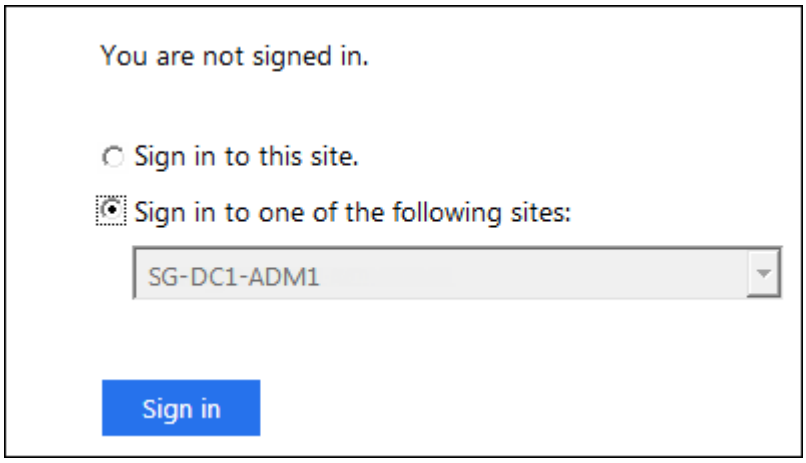
Pasos

1. Desde la página de inicio de sesión único de StorageGRID , busque el enlace en el mensaje del modo Sandbox.

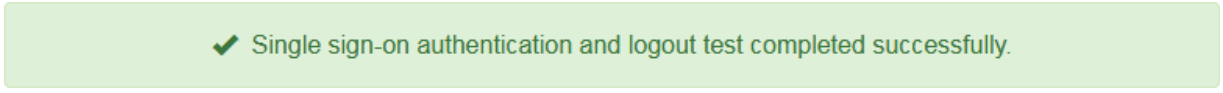
   La URL se deriva del valor ingresado en el campo **Nombre del servicio de federación**.



2. Seleccione el enlace o copie y pegue la URL en un navegador para acceder a la página de inicio de sesión de su proveedor de identidad.
3. Para confirmar que puede usar SSO para iniciar sesión en StorageGRID, seleccione * Sign in en uno de los siguientes sitios **, seleccione el identificador de parte confiable para su nodo de administración principal y seleccione * Sign in**.



4. Introduzca su nombre de usuario y contraseña federados.
   - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.



   - Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
5. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Azur

Pasos

1. Vaya a la página de inicio de sesión único en el portal de Azure.
2. Seleccione **Probar esta aplicación**.
3. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

     ✔ Single sign-on authentication and logout test completed successfully.

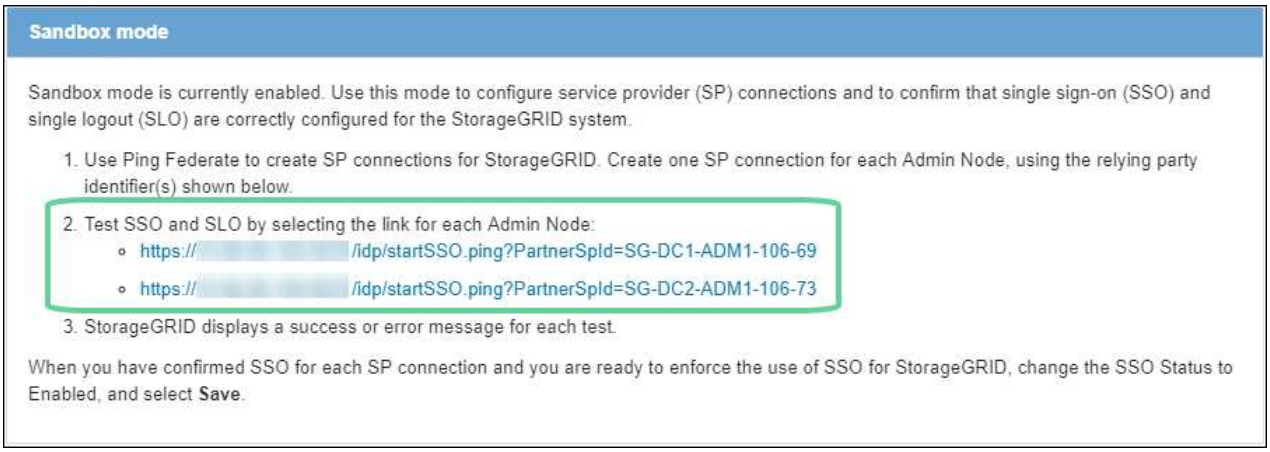
   - Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
4. Repita estos pasos para verificar la conexión SSO para cada nodo de administración en su red.

Federación de ping

Pasos

1. Desde la página de inicio de sesión único de StorageGRID , seleccione el primer enlace en el mensaje del modo Sandbox.

   Seleccione y pruebe un enlace a la vez.

2. Introduzca las credenciales de un usuario federado.
   - Si las operaciones de inicio y cierre de sesión SSO son exitosas, aparece un mensaje de éxito.

     ✔ Single sign-on authentication and logout test completed successfully.

   - Si la operación SSO no se realiza correctamente, aparece un mensaje de error. Solucione el problema, borre las cookies del navegador y vuelva a intentarlo.
3. Seleccione el siguiente enlace para verificar la conexión SSO para cada nodo de administración en su red.

   Si ve un mensaje de Página expirada, seleccione el botón **Atrás** en su navegador y vuelva a enviar sus credenciales.

Habilitar el inicio de sesión único

Cuando haya confirmado que puede usar SSO para iniciar sesión en cada nodo de administración, podrá habilitar SSO para todo su sistema StorageGRID .

> Cuando SSO está habilitado, todos los usuarios deben usar SSO para acceder al Administrador de Grid, al Administrador de inquilinos, a la API de administración de Grid y a la API de administración de inquilinos. Los usuarios locales ya no pueden acceder a StorageGRID.

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.
2. Cambie el estado de SSO a **Habilitado**.
3. Seleccione **Guardar**.
4. Revise el mensaje de advertencia y seleccione **Aceptar**.

   El inicio de sesión único ahora está habilitado.

> Si usa Azure Portal y accede a StorageGRID desde la misma computadora que usa para acceder a Azure, asegúrese de que el usuario de Azure Portal también sea un usuario autorizado de StorageGRID (un usuario en un grupo federado que se haya importado a StorageGRID) o cierre la sesión en Azure Portal antes de intentar iniciar sesión en StorageGRID.

Crear relaciones de confianza entre usuarios autenticados en AD FS

Debe utilizar los Servicios de federación de Active Directory (AD FS) para crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema. Puede crear relaciones de confianza de usuario autenticado mediante comandos de PowerShell, importando metadatos SAML desde StorageGRID o ingresando los datos manualmente.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **AD FS** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "Utilizar el modo sandbox" .
- Conoce el nombre de dominio completo (o la dirección IP) y el identificador de la parte confiable para cada nodo de administración en su sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de StorageGRID .

> Debe crear una relación de confianza de usuario autenticado para cada nodo de administración en su sistema StorageGRID . Tener una relación de confianza de parte confiable para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de relaciones de confianza de usuario autenticado en AD FS o tiene acceso a la documentación de Microsoft AD FS.
- Está utilizando el complemento Administración de AD FS y pertenece al grupo Administradores.

- Si está creando la confianza de usuario confiable manualmente, tiene el certificado personalizado que se cargó para la interfaz de administración de StorageGRID o sabe cómo iniciar sesión en un nodo de administración desde el shell de comandos.

Acerca de esta tarea

Estas instrucciones se aplican a Windows Server 2016 AD FS. Si está utilizando una versión diferente de AD FS, notará ligeras diferencias en el procedimiento. Si tiene preguntas, consulte la documentación de Microsoft AD FS.

Crear una relación de confianza de usuario autenticado mediante Windows PowerShell

Puede utilizar Windows PowerShell para crear rápidamente una o más relaciones de confianza de usuario autenticado.

Pasos

1. Desde el menú de inicio de Windows, seleccione con el botón derecho el ícono de PowerShell y seleccione **Ejecutar como administrador**.
2. En el símbolo del sistema de PowerShell, ingrese el siguiente comando:

   ```
   Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL
   "https://Admin_Node_FQDN/api/saml-metadata"
   ```

   - Para *Admin_Node_Identifier* , ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, `SG-DC1-ADM1` .
   - Para *Admin_Node_FQDN* , ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).
3. Desde el Administrador de servidor de Windows, seleccione **Herramientas** > **Administración de AD FS**.

   Aparece la herramienta de administración de AD FS.

4. Seleccione **AD FS** > **Confianzas de usuario autenticado**.

   Aparece la lista de fideicomisos de partes confiantes.

5. Agregue una Política de control de acceso a la confianza de usuario autenticado recién creada:
   a. Localice el fideicomiso de parte confiante que acaba de crear.
   b. Haga clic derecho en la confianza y seleccione **Editar política de control de acceso**.
   c. Seleccione una política de control de acceso.
   d. Seleccione **Aplicar** y seleccione **Aceptar**
6. Agregue una Política de emisión de reclamaciones al fideicomiso de parte confiada recién creado:
   a. Localice el fideicomiso de parte confiante que acaba de crear.
   b. Haga clic derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.
   c. Seleccione **Agregar regla**.
   d. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.

e. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

   Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

f. Para el almacén de atributos, seleccione **Active Directory**.

g. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.

h. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.

i. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Confirme que los metadatos se importaron correctamente.
   a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
   b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.

      Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.

8. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
9. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver"Utilizar el modo Sandbox" para obtener instrucciones.

Cree una relación de confianza entre usuarios autenticados mediante la importación de metadatos de la federación

Puede importar los valores para cada entidad de confianza accediendo a los metadatos SAML de cada nodo de administración.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Importar datos sobre la parte confiante publicados en línea o en una red local**.
5. En **Dirección de metadatos de la federación (nombre de host o URL)**, escriba la ubicación de los metadatos SAML para este nodo de administración:

   `https://Admin_Node_FQDN/api/saml-metadata`

   Para *`Admin_Node_FQDN`* , ingrese el nombre de dominio completo para el mismo nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

6. Complete el asistente de confianza de usuario autenticado, guarde la confianza de usuario autenticado y cierre el asistente.

Al ingresar el nombre para mostrar, utilice el Identificador de usuario confiado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, `SG-DC1-ADM1` .

7. Agregar una regla de reclamación:
   a. Haga clic derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.
   b. Seleccione **Agregar regla**:
   c. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.
   d. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

      Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

   e. Para el almacén de atributos, seleccione **Active Directory**.
   f. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.
   g. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.
   h. Seleccione **Finalizar** y seleccione **Aceptar**.
8. Confirme que los metadatos se importaron correctamente.
   a. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.
   b. Confirme que los campos en las pestañas **Puntos finales**, **Identificadores** y **Firma** estén completos.

      Si faltan los metadatos, confirme que la dirección de metadatos de la Federación sea correcta o ingrese los valores manualmente.

9. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
10. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver"Utilizar el modo Sandbox" para obtener instrucciones.

Crear una relación de confianza de usuario confiado manualmente

Si decide no importar los datos de las confianzas de las partes confiables, puede ingresar los valores manualmente.

Pasos

1. En el Administrador de servidor de Windows, seleccione **Herramientas** y, a continuación, seleccione **Administración de AD FS**.
2. En Acciones, seleccione **Agregar confianza de usuario autenticado**.
3. En la página de bienvenida, seleccione **Reclamos conscientes** y seleccione **Iniciar**.
4. Seleccione **Ingresar datos sobre la parte confiada manualmente** y seleccione **Siguiente**.
5. Complete el Asistente de confianza de usuario autenticado:

   a. Introduzca un nombre para mostrar para este nodo de administración.

Para mantener la coherencia, utilice el Identificador de usuario autenticado para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único en el Administrador de Grid. Por ejemplo, `SG-DC1-ADM1` .

b. Omita el paso para configurar un certificado de cifrado de token opcional.

c. En la página Configurar URL, seleccione la casilla de verificación **Habilitar soporte para el protocolo SAML 2.0 WebSSO**.

d. Escriba la URL del punto final del servicio SAML para el nodo de administración:

`https://Admin_Node_FQDN/api/saml-response`

Para *`Admin_Node_FQDN`* , ingrese el nombre de dominio completo para el nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

e. En la página Configurar identificadores, especifique el identificador de usuario de confianza para el mismo nodo de administración:

`Admin_Node_Identifier`

Para *`Admin_Node_Identifier`* , ingrese el Identificador de parte confiable para el Nodo de administración, exactamente como aparece en la página de Inicio de sesión único. Por ejemplo, `SG-DC1-ADM1` .

f. Revise la configuración, guarde la confianza del usuario autenticado y cierre el asistente.

Aparece el cuadro de diálogo Editar política de emisión de reclamaciones.

> Si el cuadro de diálogo no aparece, haga clic con el botón derecho en el fideicomiso y seleccione **Editar política de emisión de reclamaciones**.

6. Para iniciar el asistente de reglas de reclamación, seleccione **Agregar regla**:

a. En la página Seleccionar plantilla de regla, seleccione **Enviar atributos LDAP como reclamaciones** de la lista y seleccione **Siguiente**.

b. En la página Configurar regla, ingrese un nombre para mostrar para esta regla.

Por ejemplo, **ObjectGUID a ID de nombre** o **UPN a ID de nombre**.

c. Para el almacén de atributos, seleccione **Active Directory**.

d. En la columna Atributo LDAP de la tabla Mapeo, escriba **objectGUID** o seleccione **User-Principal-Name**.

e. En la columna Tipo de reclamo saliente de la tabla de mapeo, seleccione **ID de nombre** de la lista desplegable.

f. Seleccione **Finalizar** y seleccione **Aceptar**.

7. Haga clic con el botón derecho en la confianza del usuario confiado para abrir sus propiedades.

8. En la pestaña **Puntos finales**, configure el punto final para el cierre de sesión único (SLO):

a. Seleccione **Agregar SAML**.

b. Seleccione **Tipo de punto final** > **Cerrar sesión SAML**.

c. Seleccione **Enlace** > **Redireccionar**.

d. En el campo **URL de confianza**, ingrese la URL utilizada para el cierre de sesión único (SLO) desde este nodo de administración:

`https://Admin_Node_FQDN/api/saml-logout`

Para *`Admin_Node_FQDN`* , ingrese el nombre de dominio completo del nodo de administración. (Si es necesario, puede utilizar la dirección IP del nodo en su lugar. Sin embargo, si ingresa una dirección IP aquí, tenga en cuenta que debe actualizar o volver a crear esta confianza de parte confiable si esa dirección IP alguna vez cambia).

a. Seleccione **Aceptar**.

9. En la pestaña **Firma**, especifique el certificado de firma para esta relación de confianza de usuario autenticado:

a. Agregue el certificado personalizado:

- Si tiene el certificado de administración personalizado que cargó en StorageGRID, seleccione ese certificado.
- Si no tiene el certificado personalizado, inicie sesión en el Nodo de administración, vaya a `/var/local/mgmt-api` directorio del nodo de administración y agregue el `custom-server.crt` archivo de certificado.

> Uso del certificado predeterminado del nodo de administración(`server.crt`) no se recomienda. Si el nodo de administración falla, se regenerará el certificado predeterminado cuando recupere el nodo y deberá actualizar la confianza de la parte confiable.

b. Seleccione **Aplicar** y seleccione **Aceptar**.

Las propiedades de la parte confiada se guardan y cierran.

10. Repita estos pasos para configurar una relación de confianza de usuario confiable para todos los nodos de administración en su sistema StorageGRID .
11. Cuando haya terminado, regrese a StorageGRID y pruebe todas las relaciones de confianza de usuarios autenticados para confirmar que estén configuradas correctamente. Ver"Utilizar el modo sandbox" para obtener instrucciones.

Crear aplicaciones empresariales en Azure AD

Utilice Azure AD para crear una aplicación empresarial para cada nodo de administración en su sistema.

Antes de empezar

- Ha comenzado a configurar el inicio de sesión único para StorageGRID y seleccionó **Azure** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "Utilizar el modo sandbox" .
- Tiene el **nombre de la aplicación empresarial** para cada nodo de administración en su sistema. Puede copiar estos valores de la tabla de detalles del nodo de administración en la página de inicio de sesión

único de StorageGRID .

> Debe crear una aplicación empresarial para cada nodo de administración en su sistema StorageGRID . Tener una aplicación empresarial para cada nodo de administración garantiza que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo de administración.

- Tiene experiencia en la creación de aplicaciones empresariales en Azure Active Directory.
- Tiene una cuenta de Azure con una suscripción activa.
- Tiene uno de los siguientes roles en la cuenta de Azure: Administrador global, Administrador de aplicaciones en la nube, Administrador de aplicaciones o propietario de la entidad de servicio.

Acceder a Azure AD

Pasos

1. Iniciar sesión en el "Portal de Azure" .
2. Navegar a "Directorio activo de Azure" .
3. Seleccionar "Aplicaciones empresariales" .

Cree aplicaciones empresariales y guarde la configuración de SSO de StorageGRID

Para guardar la configuración de SSO para Azure en StorageGRID, debe usar Azure para crear una aplicación empresarial para cada nodo de administración. Copiará las URL de metadatos de federación de Azure y las pegará en los campos **URL de metadatos de federación** correspondientes en la página de inicio de sesión único de StorageGRID .

Pasos

1. Repita los siguientes pasos para cada nodo de administración.
   a. En el panel de aplicaciones empresariales de Azure, seleccione **Nueva aplicación**.
   b. Seleccione **Crea tu propia aplicación**.
   c. Para el nombre, ingrese el **nombre de la aplicación empresarial** que copió de la tabla de detalles del nodo de administración en la página de inicio de sesión único de StorageGRID .
   d. Deje seleccionado el botón de opción **Integrar cualquier otra aplicación que no encuentre en la galería (No galería)**.
   e. Seleccione **Crear**.
   f. Seleccione el enlace **Comenzar** en el **2. Configurar el cuadro de inicio de sesión único** o seleccione el enlace **Inicio de sesión único** en el margen izquierdo.
   g. Seleccione la casilla **SAML**.
   h. Copie la **URL de metadatos de federación de aplicaciones**, que puede encontrar en el **Paso 3 Certificado de firma SAML**.
   i. Vaya a la página de inicio de sesión único de StorageGRID y pegue en el campo **URL de metadatos de federación** la URL que corresponde al **nombre de la aplicación empresarial** que utilizó.
2. Después de haber pegado una URL de metadatos de federación para cada nodo de administración y realizado todos los demás cambios necesarios en la configuración de SSO, seleccione **Guardar** en la página de inicio de sesión único de StorageGRID .

Descargar metadatos SAML para cada nodo de administración

Una vez guardada la configuración de SSO, puede descargar un archivo de metadatos SAML para cada nodo de administración en su sistema StorageGRID .

Pasos

1. Repita estos pasos para cada nodo de administración.
   a. Sign in en StorageGRID desde el nodo de administración.
   b. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.
   c. Seleccione el botón para descargar los metadatos SAML para ese nodo de administración.
   d. Guarde el archivo que cargará en Azure AD.

Cargar metadatos SAML a cada aplicación empresarial

Después de descargar un archivo de metadatos SAML para cada nodo de administración de StorageGRID , realice los siguientes pasos en Azure AD:

Pasos

1. Regresar al Portal de Azure.
2. Repita estos pasos para cada aplicación empresarial:

   > Es posible que necesites actualizar la página de aplicaciones empresariales para ver las aplicaciones que agregaste previamente a la lista.

   a. Vaya a la página Propiedades de la aplicación empresarial.
   b. Establezca **Tarea requerida** en **No** (a menos que desee configurar las asignaciones por separado).
   c. Vaya a la página de inicio de sesión único.
   d. Complete la configuración de SAML.
   e. Seleccione el botón **Cargar archivo de metadatos** y seleccione el archivo de metadatos SAML que descargó para el nodo de administración correspondiente.
   f. Después de cargar el archivo, seleccione **Guardar** y luego seleccione **X** para cerrar el panel. Regresará a la página Configurar inicio de sesión único con SAML.
3. Siga los pasos en"Utilizar el modo sandbox" para probar cada aplicación.

Crear conexiones de proveedor de servicios (SP) en PingFederate

Utilice PingFederate para crear una conexión de proveedor de servicios (SP) para cada nodo de administración en su sistema. Para acelerar el proceso, importará los metadatos SAML desde StorageGRID.

Antes de empezar

- Ha configurado el inicio de sesión único para StorageGRID y seleccionó **Ping Federate** como tipo de SSO.
- El **modo Sandbox** está seleccionado en la página de inicio de sesión único en Grid Manager. Ver "Utilizar el modo sandbox" .
- Tienes el *ID de conexión SP * para cada nodo de administración en tu sistema. Puede encontrar estos valores en la tabla de detalles de Nodos de administración en la página de inicio de sesión único de

StorageGRID .

- Ha descargado los **metadatos SAML** para cada nodo de administración en su sistema.
- Tiene experiencia en la creación de conexiones SP en PingFederate Server.
- Tú tienes elhttps://docs.pingidentity.com/pingfederate/latest/administrators_reference_guide/pf_administrators_reference_guide.html["Guía de referencia del administrador"^] para el servidor PingFederate. La documentación de PingFederate proporciona instrucciones y explicaciones detalladas paso a paso.
- Tú tienes el"Permiso de administrador" para el servidor PingFederate.

Acerca de esta tarea

Estas instrucciones resumen cómo configurar PingFederate Server versión 10.3 como proveedor de SSO para StorageGRID. Si está utilizando otra versión de PingFederate, es posible que deba adaptar estas instrucciones. Consulte la documentación del servidor PingFederate para obtener instrucciones detalladas para su versión.

Requisitos previos completos en PingFederate

Antes de poder crear las conexiones SP que utilizará para StorageGRID, debe completar las tareas previas requeridas en PingFederate. Utilizará la información de estos requisitos previos cuando configure las conexiones del SP .

Crear almacén de datos[[almacén de datos]]

Si aún no lo ha hecho, cree un almacén de datos para conectar PingFederate al servidor LDAP de AD FS. Utilice los valores que utilizó cuando"configuración de la federación de identidades" en StorageGRID.

- **Tipo**: Directorio (LDAP)
- **Tipo LDAP**: Directorio activo
- **Nombre del atributo binario**: Ingrese **objectGUID** en la pestaña Atributos binarios LDAP exactamente como se muestra.

Crear un validador de credenciales de contraseña

Si aún no lo ha hecho, cree un validador de credenciales de contraseña.

- **Tipo**: LDAP Nombre de usuario Contraseña Credencial Validador
- **Almacén de datos**: seleccione el almacén de datos que creó.
- **Base de búsqueda**: Ingrese información de LDAP (por ejemplo, DC=saml,DC=sgws).
- **Filtro de búsqueda**: sAMAccountName=${username}
- **Alcance**: Subárbol

Crear una instancia de adaptador de IdP

Si aún no lo ha hecho, cree una instancia de adaptador IdP.

Pasos

1. Vaya a **Autenticación** > **Integración** > **Adaptadores IdP**.
2. Seleccione **Crear nueva instancia**.
3. En la pestaña Tipo, seleccione **Adaptador IdP de formulario HTML**.

4. En la pestaña Adaptador IdP, seleccione **Agregar una nueva fila a 'Validadores de credenciales'**.
5. Seleccione elvalidador de credenciales de contraseña tu creaste
6. En la pestaña Atributos del adaptador, seleccione el atributo **nombre de usuario** para **Seudónimo**.
7. Seleccione **Guardar**.

Crear o importar certificado de firma

Si aún no lo ha hecho, cree o importe el certificado de firma.

Pasos

1. Vaya a **Seguridad** > **Claves y certificados de firma y descifrado**.
2. Cree o importe el certificado de firma.

Crear una conexión SP en PingFederate

Cuando crea una conexión SP en PingFederate, importa los metadatos SAML que descargó de StorageGRID para el nodo de administración. El archivo de metadatos contiene muchos de los valores específicos que necesita.

> Debe crear una conexión SP para cada nodo de administración en su sistema StorageGRID , de modo que los usuarios puedan iniciar y cerrar sesión de forma segura en cualquier nodo. Utilice estas instrucciones para crear la primera conexión SP . Luego, ve aCrear conexiones SP adicionales para crear cualquier conexión adicional que necesites.

Elija el tipo de conexión SP

Pasos

1. Vaya a **Aplicaciones** > **Integración** > *Conexiones SP *.
2. Seleccione **Crear conexión**.
3. Seleccione **No utilizar una plantilla para esta conexión**.
4. Seleccione **Perfiles SSO del navegador** y **SAML 2.0** como protocolo.

Importar metadatos de SP

Pasos

1. En la pestaña Importar metadatos, seleccione **Archivo**.
2. Elija el archivo de metadatos SAML que descargó de la página de inicio de sesión único de StorageGRID para el nodo de administración.
3. Revise el Resumen de metadatos y la información proporcionada en la pestaña Información general.

   El ID de entidad del socio y el nombre de la conexión se establecen en el ID de conexión de StorageGRID SP . (por ejemplo, 10.96.105.200-DC1-ADM1-105-200). La URL base es la IP del nodo de administración de StorageGRID .

4. Seleccione **Siguiente**.

Configurar el inicio de sesión único (SSO) del navegador IdP

Pasos

1. Desde la pestaña SSO del navegador, seleccione **Configurar SSO del navegador**.
2. En la pestaña Perfiles SAML, seleccione las opciones * SP-initiated SSO*, * SP-initial SLO*, **IdP-initiated SSO** y **IdP-initiated SLO**.
3. Seleccione **Siguiente**.
4. En la pestaña Duración de la afirmación, no realice cambios.
5. En la pestaña Creación de aserciones, seleccione **Configurar creación de aserciones**.
   a. En la pestaña Asignación de identidad, seleccione **Estándar**.
   b. En la pestaña Contrato de atributo, utilice **SAML_SUBJECT** como Contrato de atributo y el formato de nombre no especificado que se importó.
6. Para extender el contrato, seleccione **Eliminar** para quitar el `urn:oid` , que no se utiliza.

Instancia del adaptador de mapas

Pasos

1. En la pestaña Mapeo de origen de autenticación, seleccione **Asignar nueva instancia de adaptador**.
2. En la pestaña Instancia del adaptador, seleccione lainstancia de adaptador tu creaste
3. En la pestaña Método de mapeo, seleccione **Recuperar atributos adicionales de un almacén de datos**.
4. En la pestaña Origen de atributos y búsqueda de usuarios, seleccione **Agregar origen de atributos**.
5. En la pestaña Almacén de datos, proporcione una descripción y seleccione laalmacén de datos usted agregó.
6. En la pestaña Búsqueda de directorio LDAP:
   - Ingrese el **DN base**, que debe coincidir exactamente con el valor ingresado en StorageGRID para el servidor LDAP.
   - Para el ámbito de búsqueda, seleccione **Subárbol**.
   - Para la clase de objeto raíz, busque y agregue cualquiera de estos atributos: **objectGUID** o **userPrincipalName**.
7. En la pestaña Tipos de codificación de atributos binarios LDAP, seleccione **Base64** para el atributo **objectGUID**.
8. En la pestaña Filtro LDAP, ingrese **sAMAccountName=${username}**.
9. En la pestaña Cumplimiento de contrato de atributo, seleccione **LDAP (atributo)** en el menú desplegable Fuente y seleccione **objectGUID** o **userPrincipalName** en el menú desplegable Valor.
10. Revise y luego guarde la fuente del atributo.
11. En la pestaña Origen del atributo de guardado fallido, seleccione **Anular la transacción SSO**.
12. Revise el resumen y seleccione **Listo**.
13. Seleccione **Listo**.

Configurar los ajustes del protocolo

Pasos

1. En la pestaña **Conexión SP * > *SSO del navegador** > **Configuración del protocolo**, seleccione **Configurar configuración del protocolo**.
2. En la pestaña URL del servicio de consumidor de aserciones, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**POST** para enlace y `/api/saml-response` para la

URL del punto final).

3. En la pestaña URL del servicio SLO, acepte los valores predeterminados, que se importaron de los metadatos SAML de StorageGRID (**REDIRECT** para enlace y `/api/saml-logout` para URL de punto final.
4. En la pestaña Enlaces SAML permitidos, desactive **ARTIFACT** y **SOAP**. Sólo se requieren **POST** y **REDIRECT**.
5. En la pestaña Política de firma, deje seleccionadas las casillas de verificación **Requerir que las solicitudes de autenticación estén firmadas** y **Firmar siempre la afirmación**.
6. En la pestaña Política de cifrado, seleccione **Ninguno**.
7. Revise el resumen y seleccione **Listo** para guardar la configuración del protocolo.
8. Revise el resumen y seleccione **Listo** para guardar la configuración de SSO del navegador.

Configurar credenciales

Pasos

1. Desde la pestaña Conexión SP , seleccione **Credenciales**.
2. Desde la pestaña Credenciales, seleccione **Configurar credenciales**.
3. Seleccione elcertificado de firma usted creó o importó.
4. Seleccione **Siguiente** para ir a **Administrar configuración de verificación de firma**.
   a. En la pestaña Modelo de confianza, seleccione **Sin ancla**.
   b. En la pestaña Certificado de verificación de firma, revise la información del certificado de firma, que se importó de los metadatos SAML de StorageGRID .
5. Revise las pantallas de resumen y seleccione **Guardar** para guardar la conexión SP .

Crear conexiones SP adicionales

Puede copiar la primera conexión SP para crear las conexiones SP que necesita para cada nodo de administración en su red. Carga nuevos metadatos para cada copia.

> Las conexiones SP para diferentes nodos de administración utilizan configuraciones idénticas, con la excepción del ID de entidad del socio, la URL base, el ID de conexión, el nombre de la conexión, la verificación de firma y la URL de respuesta de SLO.

Pasos

1. Seleccione **Acción** > **Copiar** para crear una copia de la conexión SP inicial para cada nodo de administración adicional.
2. Ingrese el ID de conexión y el nombre de conexión para la copia y seleccione **Guardar**.
3. Seleccione el archivo de metadatos correspondiente al Nodo de Administración:
   a. Seleccione **Acción** > **Actualizar con metadatos**.
   b. Seleccione **Elegir archivo** y cargue los metadatos.
   c. Seleccione **Siguiente**.
   d. Seleccione **Guardar**.
4. Resuelva el error debido al atributo no utilizado:
   a. Seleccione la nueva conexión.

b. Seleccione **Configurar SSO del navegador > Configurar creación de afirmaciones > Contrato de atributos**.

c. Eliminar la entrada para **urn:oid**.

d. Seleccione **Guardar**.

Deshabilitar el inicio de sesión único

Puede desactivar el inicio de sesión único (SSO) si ya no desea utilizar esta funcionalidad. Debe deshabilitar el inicio de sesión único antes de poder deshabilitar la federación de identidad.

Antes de empezar

- Ha iniciado sesión en Grid Manager mediante un"navegador web compatible" .
- Tienes"permisos de acceso específicos" .

Pasos

1. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.

   Aparece la página de inicio de sesión único.

2. Seleccione la opción **Deshabilitado**.
3. Seleccione **Guardar**.

   Aparece un mensaje de advertencia que indica que los usuarios locales ahora podrán iniciar sesión.

4. Seleccione **Aceptar**.

   La próxima vez que inicie sesión en StorageGRID , aparecerá la página de Sign in de StorageGRID y deberá ingresar el nombre de usuario y la contraseña de un usuario de StorageGRID local o federado.

Deshabilitar temporalmente y volver a habilitar el inicio de sesión único para un nodo de administración

Es posible que no pueda iniciar sesión en Grid Manager si el sistema de inicio de sesión único (SSO) deja de funcionar. En este caso, puede deshabilitar y volver a habilitar temporalmente el SSO para un nodo de administración. Para deshabilitar y luego volver a habilitar SSO, debe acceder al shell de comandos del nodo.

Antes de empezar

- Tienes"permisos de acceso específicos" .
- Tú tienes el `Passwords.txt` archivo.
- Conoces la contraseña del usuario root local.

Acerca de esta tarea

Después de deshabilitar SSO para un nodo de administración, puede iniciar sesión en Grid Manager como usuario raíz local. Para proteger su sistema StorageGRID , debe usar el shell de comandos del nodo para volver a habilitar SSO en el nodo de administración tan pronto como cierre la sesión.

Deshabilitar SSO para un nodo de administración no afecta la configuración de SSO de ningún otro nodo de administración en la red. La casilla de verificación **Habilitar SSO** en la página de Inicio de sesión único en el Administrador de Grid permanece seleccionada y todas las configuraciones de SSO existentes se mantienen a menos que las actualice.

Pasos

1. Inicie sesión en un nodo de administración:
   a. Introduzca el siguiente comando: `ssh admin@Admin_Node_IP`
   b. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.
   c. Introduzca el siguiente comando para cambiar a root: `su -`
   d. Introduzca la contraseña que aparece en el `Passwords.txt` archivo.

      Cuando inicia sesión como root, el mensaje cambia de `$` a `#` .

2. Ejecute el siguiente comando:`disable-saml`

   Un mensaje indica que el comando se aplica únicamente a este nodo de administración.

3. Confirme que desea deshabilitar SSO.

   Un mensaje indica que el inicio de sesión único está deshabilitado en el nodo.

4. Desde un navegador web, acceda al Administrador de cuadrícula en el mismo nodo de administración.

   Ahora se muestra la página de inicio de sesión de Grid Manager porque se ha deshabilitado el SSO.

5. Sign in con el nombre de usuario root y la contraseña del usuario root local.
6. Si deshabilitó SSO temporalmente porque necesitaba corregir la configuración de SSO:
   a. Seleccione **CONFIGURACIÓN** > **Control de acceso** > **Inicio de sesión único**.
   b. Cambie la configuración de SSO incorrecta o desactualizada.
   c. Seleccione **Guardar**.

      Al seleccionar **Guardar** en la página de inicio de sesión único, se vuelve a habilitar automáticamente el SSO para toda la red.

7. Si deshabilitó el SSO temporalmente porque necesitaba acceder al Administrador de Grid por algún otro motivo:
   a. Realice cualquier tarea o tareas que necesite realizar.
   b. Seleccione **Cerrar sesión** y cierre el Administrador de cuadrícula.
   c. Vuelva a habilitar SSO en el nodo de administración. Puede realizar cualquiera de los siguientes pasos:

      - Ejecute el siguiente comando: `enable-saml`

        Un mensaje indica que el comando se aplica únicamente a este nodo de administración.

      Confirme que desea habilitar SSO.

Un mensaje indica que el inicio de sesión único está habilitado en el nodo.

    - Reiniciar el nodo de la red: `reboot`

8. Desde un navegador web, acceda al Administrador de cuadrícula desde el mismo nodo de administración.
9. Confirme que aparezca la página de Sign in de StorageGRID y que debe ingresar sus credenciales de SSO para acceder al Administrador de Grid.